

No title available

Publication number: JP2003158514 (A)

Publication date: 2003-05-30

Inventor(s):

Applicant(s):

Classification:


- international: **G06F12/14; G06F21/06; G06F21/24; G06K17/00; G06K19/00; G06K19/10; G09C1/00; G11B20/10; H04L9/08; H04N5/765; H04N5/91; H04N5/93; G06F12/14; G06F21/00; G06K17/00; G06K19/00; G06K19/10; G09C1/00; G11B20/10; H04L9/08; H04N5/765; H04N5/91; H04N5/93; (IPC1-7): G06F12/14; G06K17/00; G06K19/00; G06K19/10; G09C1/00; G11B20/10; H04L9/08; H04N5/765; H04N5/91; H04N5/93**

- European:

Application number: JP20020199142 20020708

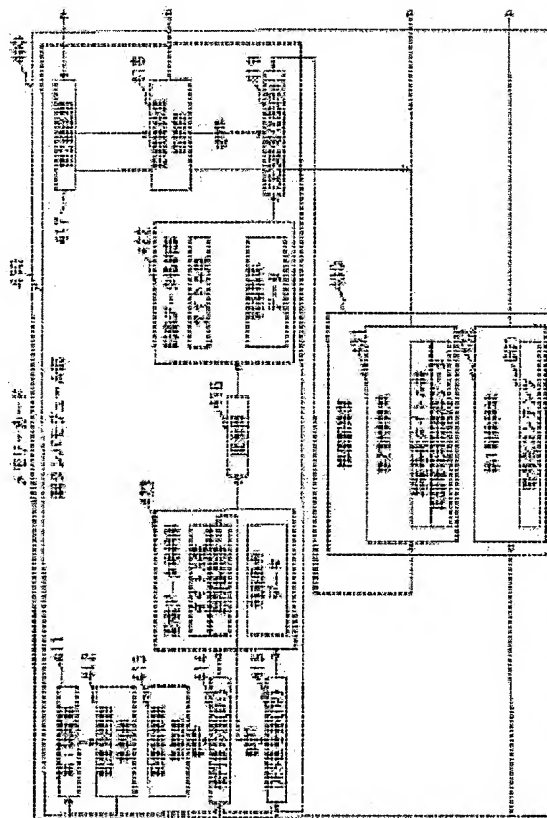
Priority number(s): JP20020199142 20020708; JP20010208533 20010709

Also published as:

 **JP4224262 (B2)**

Abstract of JP 2003158514 (A)

PROBLEM TO BE SOLVED: To provide a digital work protection system that makes hacking difficult without increasing the size of the computer program and without slowing down the performance of the computer. **SOLUTION:** A server apparatus encrypts contents on the basis of a distraction key, and transmits the encrypted contents to a PC via a network. The PC, to which a memory card is connected, outputs the received encrypted contents to the memory card. The memory card decrypts the encrypted contents using the distribution key, converts the data format of the decrypted contents, encrypts the contents using a medium unique key that is unique to the memory card, and records the resulting re-encrypted contents internally. A playback apparatus decrypts the re-encrypted contents using the medium unique key, and plays back the decrypted contents.



Data supplied from the **espacenet** database — Worldwide

(11)特許出願公開番号

特開2003-158514

(P2003-158514A)

(43)公開日 平成15年5月30日(2003.5.30)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 K 17/00	D 5 B 0 3 5
G 0 6 K 17/00			L 5 B 0 5 8
			T 5 C 0 5 3
		G 0 9 C 1/00	6 6 0 A 5 D 0 4 4
審査請求 未請求 請求項の数32 O L (全 40 頁) 最終頁に続く			

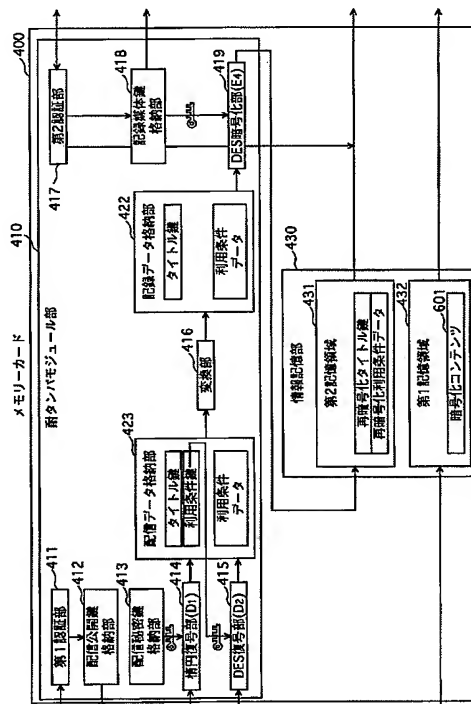
[最終頁に続く](#)

(54) 【発明の名称】 デジタル著作物保護システム、記録媒体装置、送信装置及び再生装置

(57) 【要約】

【課題】 プログラムの量が増加することなく、速度性能が低下することなく、ハッキングを困難にするデジタル著作物保護システムを提供する。

【解決手段】サーバ装置は、コンテンツを配信鍵に基づいて暗号化し、ネットワークを介してＰＣへ送信する。ＰＣにメモリカードが装着され、ＰＣは、受信した暗号化コンテンツをメモリカードへ出力する。メモリカードは、配信鍵を用いて暗号化コンテンツを復号し、さらにデータ形式を変換し、メモリカードに固有の媒体固有鍵を用いて暗号化して内部に記録する。再生装置は、再度暗号化されたコンテンツを前記媒体固有鍵を用いて復号して再生する。



【特許請求の範囲】

【請求項 1】 送信装置から送信されたデジタル著作物を、受信装置を介して、可搬型の記録媒体装置に書き込み、再生装置により再生するデジタル著作物保護システムであって、

前記デジタル著作物保護システムは、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第 1 暗号化情報を生成し、生成した第 1 暗号化情報をネットワークを介して送信する前記送信装置を含み、

ここで、前記記録媒体装置が前記受信装置に装着され、前記デジタル著作物保護システムは、さらに、ネットワークを介して前記第 1 暗号化情報を受信し、受信した前記第 1 暗号化情報を前記記録媒体装置へ出力する受信装置と、

情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タンパモジュール部とを備える前記記録媒体装置とを含み、

前記耐タンパモジュール部は、出力された前記第 1 暗号化情報を取得し、配信復号鍵に基づいて前記第 1 暗号化情報を復号して中間情報を生成し、前記記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第 2 暗号化情報を生成し、生成した第 2 暗号化情報を前記情報記憶領域に書き込み、

ここで、前記第 2 暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、

前記デジタル著作物保護システムは、さらに、前記情報記憶領域から前記第 2 暗号化情報を読み出し、前記媒体固有鍵をセキュアに読み出し、前記媒体固有鍵に基づいて前記第 2 暗号化情報を復号して復号コンテンツを生成し、生成した復号コンテンツを再生する前記再生装置を含むことを特徴とするデジタル著作物保護システム。

【請求項 2】 前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる前記配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した前記配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツと第 1 暗号化コンテンツ鍵とを含む前記第 1 暗号化情報を送信し、

前記受信装置は、前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を受信し、受信した前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を出力し、

前記耐タンパモジュール部は、配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶しており、出力された前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を取得し、前記配信復号鍵を用いて、前記第 1 暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記媒体固有鍵を用いて、

生成した前記中間コンテンツ鍵を暗号化して第 2 暗号化コンテンツ鍵を生成し、取得した前記暗号化コンテンツと生成した前記第 2 暗号化コンテンツ鍵とを含む前記第 2 暗号化情報を書き込み、

前記再生装置は、前記記録媒体装置から前記媒体固有鍵をセキュアに取得し、前記情報記憶領域から、前記暗号化コンテンツと前記第 2 暗号化コンテンツ鍵とを含む前記第 2 暗号化情報を読み出し、取得した前記媒体固有鍵を用いて、前記第 2 暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成することを特徴とする請求項 1 に記載のデジタル著作物保護システム。

【請求項 3】 デジタル著作物を送信する送信装置と、ネットワークを介して受信した前記デジタル著作物を可搬型の記録媒体装置に記録する受信装置と、前記記録媒体装置に記録された前記デジタル著作物を再生する再生装置と、前記記録媒体装置とから構成されるデジタル著作物保護システムであって、

前記送信装置は、デジタル著作物である原コンテンツと当該原コンテンツに固有の原コンテンツ鍵を予め記憶している記憶手段と、

デジタル著作物の配信のために用いられる配信暗号鍵を取得する配信暗号鍵取得手段と、

前記原コンテンツ鍵を用いて、前記原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成する暗号化手段と、

前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を、ネットワークを介して、送信する送信手段とを含み、

ここで、前記記録媒体装置が前記受信装置に装着され、前記受信装置は、

ネットワークを介して前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を受信する受信手段と、

受信した前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を出力する出力手段とを含み、

前記記録媒体装置は、

情報を記憶するための領域を備えている情報記憶手段と、

耐タンパ性を有する耐タンパモジュール手段とを含み、前記耐タンパモジュール手段は、

配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶している鍵記憶部と、

出力された前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を取得する取得部と、

前記配信復号鍵を用いて、前記第 1 暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成する復号部と、

前記媒体固有鍵を用いて、生成した前記中間コンテンツ

鍵を暗号化して第 2 暗号化コンテンツ鍵を生成する暗号化部と、

取得した前記暗号化コンテンツ及び生成した前記第 2 暗号化コンテンツ鍵を前記情報記憶手段に書き込む書込部とを含み、

ここで、前記暗号化コンテンツ及び前記第 2 暗号化コンテンツ鍵が書き込まれた前記記録媒体装置が前記再生装置に装着され、

前記再生装置は、

前記鍵記憶部から前記媒体固有鍵をセキュアに取得する鍵取得手段と、

前記情報記憶手段から前記暗号化コンテンツと前記第 2 暗号化コンテンツ鍵とを読み出す読出手段と、

取得した前記媒体固有鍵を用いて、読み出した前記第 2 暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成するコンテンツ鍵復号手段と、

生成された前記復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成するコンテンツ復号手段と、

生成された復号コンテンツを再生する再生手段とを備えることを特徴とするデジタル著作物保護システム。

【請求項 4】 デジタル著作物をネットワークを介して送信する送信装置であって、

前記デジタル著作物は、受信装置を介して、可搬型の記録媒体装置に書き込まれ、

前記送信装置は、

デジタル著作物である原コンテンツと当該原コンテンツに固有の原コンテンツ鍵を予め記憶している記憶手段と、

デジタル著作物の配信のために用いられる配信暗号鍵を取得する配信暗号鍵取得手段と、

前記原コンテンツ鍵を用いて、前記原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成する暗号化手段と、

前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を、ネットワークを介して、送信する送信手段とを備えることを特徴とする送信装置。

【請求項 5】 前記記憶手段は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、

前記暗号化手段は、さらに、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第 1 暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第 1 暗号化利用条件情報を生成し、

前記送信手段は、さらに、前記第 1 暗号化利用条件鍵及び前記第 1 暗号化利用条件情報を、ネットワークを介して、送信することを特徴とする請求項 4 に記載の送信装置。

【請求項 6】 前記配信暗号鍵取得手段は、公開鍵生成

アルゴリズムを用いて生成された公開鍵である前記配信暗号鍵を取得し、

前記暗号化手段は、公開鍵である配信暗号鍵を用いて、公開鍵暗号アルゴリズムにより、暗号化することの特徴とする請求項 5 に記載の送信装置。

【請求項 7】 前記送信装置は、さらに、

無効の配信暗号鍵を記録するための領域を備えるリポークリスト手段と、

公開鍵である前記配信暗号鍵の生成において基にされた配信復号鍵が暴露された場合に、前記配信暗号鍵を前記リポークリスト手段に書き込む登録手段とを含み、

ここで、前記送信装置は、新たにデジタル著作物であるコンテンツを送信し、

前記配信鍵取得手段は、新たに配信暗号鍵を取得し、取得した配信暗号鍵がリポークリスト手段に書き込まれているか否かを判断し、書き込まれていると判断する場合には、前記暗号化手段に対して暗号化を禁止し、前記送信手段に対して送信を禁止することを特徴とする請求項 6 に記載の送信装置。

【請求項 8】 前記記憶手段は、さらに、前記デジタル著作物の利用条件を示す利用条件情報を記憶しており、前記送信手段は、さらに、前記記憶手段から前記利用条件情報を読み出し、読み出した前記利用条件情報にハッシュアルゴリズムを施してハッシュ値を生成し、生成した前記ハッシュ値と読み出した利用条件情報を、セキュアにネットワークを介して送信することを特徴とする請求項 4 に記載の送信装置。

【請求項 9】 前記送信装置は、さらに、

前記記録媒体装置との間で相互に機器の正当性を認証する認証手段を含み、

前記配信暗号鍵取得手段は、前記認証に成功した場合にのみ、前記配信暗号鍵を前記記録媒体装置から取得し、前記暗号化手段は、前記認証に成功した場合にのみ、暗号化し、

前記送信手段は、前記認証に成功した場合にのみ、送信することを特徴とする請求項 4 に記載の送信装置。

【請求項 10】 前記送信装置は、さらに、

前記記録媒体装置が備える耐タンパモジュール部を更新するための更新情報を予め記憶している更新情報記憶手段と、

前記更新情報記憶手段から前記更新情報を読み出し、読み出した前記更新情報を、ネットワーク及び受信装置を介して、前記記録媒体装置へ送信する更新情報送信手段とを含むことを特徴とする請求項 4 に記載の送信装置。

【請求項 11】 前記送信装置は、さらに、

前記更新情報記憶手段から前記更新情報を読み出し、読み出した更新情報にハッシュアルゴリズムを施してハッシュ値を生成し、生成したハッシュ値を、ネットワーク及び受信装置を介して、前記記録媒体装置へセキュアに送信するハッシュ手段を含むことを特徴とする請求項 1

0に記載の送信装置。

【請求項12】 前記更新情報記憶手段が記憶している更新情報は、前記耐タンパモジュール部が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含み、前記更新情報送信手段は、前記耐タンパモジュール部が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含む前記更新情報を読み出し、読み出した前記更新情報を送信することを特徴とする請求項11に記載の送信装置。

【請求項13】 送信装置から送信されたデジタル著作物を、受信装置を介して、記録する可搬型の記録媒体装置であって、前記記録媒体装置が前記受信装置に装着され、前記送信装置は、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報を、ネットワークを介して、前記受信装置へ送信し、前記記録媒体装置は、情報を記憶するための領域を備える情報記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備え、前記耐タンパモジュール手段は、配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶している鍵記憶部と、前記受信装置を介して、送信された前記第1暗号化情報を取得する取得部と、前記配信復号鍵に基づいて前記第1暗号化情報を復号して中間情報を生成する復号部と、前記媒体固有鍵に基づいて前記中間情報を暗号化して第2暗号化情報を生成する暗号化部と、生成した第2暗号化情報を前記情報記憶手段に書き込む書込部とを備えることを特徴とする記録媒体装置。

【請求項14】 前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第1暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ及び第1暗号化コンテンツ鍵を含む前記第1暗号化情報を送信し、前記取得部は、出力された前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を含む前記第1暗号化情報を取得し、前記復号部は、前記配信復号鍵を用いて、前記第1暗号化情報に含まれる前記第1暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記第1暗号化情報に含まれる前記暗号化コンテンツ及び生成した前記中間コンテンツ鍵を含む前記中間情報を生成し、

前記暗号化部は、前記媒体固有鍵を用いて、前記中間情報に含まれる前記中間コンテンツ鍵を暗号化して第2暗号化コンテンツ鍵を生成し、前記中間情報に含まれる前記暗号化コンテンツ及び生成した前記第2暗号化コンテンツ鍵を含む前記第2暗号化情報を生成し、前記書込部は、前記暗号化コンテンツ及び前記第2暗号化コンテンツ鍵を含む前記第2暗号化情報を書き込むことを特徴とする請求項13に記載の記録媒体装置。

【請求項15】 前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第1暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第1暗号化利用条件情報を生成し、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を、ネットワークを介して、前記受信装置へ送信し、前記取得部は、さらに、前記受信装置を介して、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を取得し、前記復号部は、さらに、前記配信復号鍵を用いて、前記第1暗号化利用条件鍵を復号して中間利用条件鍵を生成し、生成した前記中間利用条件鍵を用いて、前記第1暗号化利用条件情報を復号して、中間利用条件情報を生成し、前記暗号化部は、さらに、前記媒体固有鍵を用いて、前記中間利用条件情報を暗号化して第2暗号化利用条件情報を生成し、前記書込部は、さらに、生成した第2暗号化利用条件情報を前記情報記憶手段に書き込むことを特徴とする請求項14に記載の記録媒体装置。

【請求項16】 前記送信装置は、さらに、秘密鍵である配信用復号鍵を基にして公開鍵生成アルゴリズムを用いて生成された公開鍵である前記配信暗号鍵を取得し、公開鍵である配信暗号鍵を用いて、公開鍵暗号アルゴリズムにより、暗号化し、前記復号部は、公開鍵復号アルゴリズムにより、前記配信用復号鍵を用いて復号することを特徴とする請求項15に記載の記録媒体装置。

【請求項17】 前記耐タンパモジュール手段は、さらに、前記復号部により生成された配信データ形式である前記中間情報を変換して、記録データ形式の記録中間情報を生成する変換部を含み、前記暗号化部は、前記中間情報に代えて、前記記録中間情報を暗号化することを特徴とする請求項14に記載の記録媒体装置。

【請求項18】 前記送信装置は、前記記録媒体装置が備える前記耐タンパモジュール手段を更新するための更

新情報を予め記憶しており、前記更新情報を読み出し、読み出した前記更新情報を、ネットワーク及び受信装置を介して、前記記録媒体装置へ送信し、前記耐タンパモジュール手段は、マイクロプロセッサとコンピュータプログラムを記録している半導体メモリを含み、前記コンピュータプログラムに従って、前記マイクロプロセッサが動作することにより、前記耐タンパモジュール手段に含まれる構成要素が動作し、前記取得部は、前記受信装置を介して、前記更新情報を取得し、前記耐タンパモジュール手段は、さらに、取得した前記更新情報を用いて、前記コンピュータプログラムを更新し、これにより、前記耐タンパモジュール手段に含まれる構成要素が更新される更新部を含むことを特徴とする請求項 17 に記載の記録媒体装置。

【請求項 19】 前記送信装置は、さらに、前記更新情報を読み出し、読み出した更新情報にハッシュアルゴリズムを施して第 1 ハッシュ値を生成し、生成した第 1 ハッシュ値を、ネットワーク及び受信装置を介して、前記記録媒体装置へセキュアに送信し、前記耐タンパモジュール手段は、さらに、取得した前記更新情報に前記ハッシュアルゴリズムを施して第 2 ハッシュ値を生成するハッシュ部と、取得した前記第 1 ハッシュ値と生成した前記第 2 ハッシュ値とが一致するか否かを判断する比較判断部とを含み、前記更新部は、前記比較判断部により一致すると判断された場合にのみ、更新することを特徴とする請求項 18 に記載の記録媒体装置。

【請求項 20】 前記送信装置が記憶している更新情報は、前記耐タンパモジュール手段が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含み、前記前記更新情報を送信し、前記取得部は、暗号化方式、復号方式、又はデータ変換方式を更新するための前記更新情報を前記受信装置を介して取得し、前記更新部は、取得した前記更新情報を用いて、前記コンピュータプログラムを更新し、これにより、前記耐タンパモジュール手段に含まれる暗号化部、復号部、又は変換部が更新されることを特徴とする請求項 19 に記載の記録媒体装置。

【請求項 21】 前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報を記憶しており、前記利用条件情報を読み出し、読み出した前記利用条件情報にハッシュアルゴリズムを施して第 1 ハッシュ値を生成し、生成した前記第 1 ハッシュ値と読み出した利用条件情報を、ネットワークを介してセキュアに送信し、前記取得部は、さらに、前記受信装置を介して、送信さ

れた前記第 1 ハッシュ値と前記利用条件情報とを取得し、前記耐タンパモジュール手段は、さらに、取得した前記利用条件情報に前記ハッシュアルゴリズムを施して第 2 ハッシュ値を生成するハッシュ部と、取得した前記第 1 ハッシュ値と生成した前記第 2 ハッシュ値とが一致するか否かを判断する比較判断部とを含み、前記暗号化部は、前記比較判断部により一致すると判断された場合にのみ、暗号化し、前記書込部は、前記比較判断部により一致すると判断された場合にのみ、書き込むことを特徴とする請求項 14 に記載の記録媒体装置。

【請求項 22】 前記送信装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証し、前記認証に成功した場合にのみ、前記配信暗号鍵を前記記録媒体装置から取得し、暗号化し、送信し、前記耐タンパモジュール手段は、さらに、前記送信装置との間で相互に機器の正当性を認証する認証手段を含み、前記取得部は、前記認証に成功した場合にのみ、取得し、前記復号部は、前記認証に成功した場合にのみ、復号し、前記暗号化部は、前記認証に成功した場合にのみ、暗号化し、前記書込部は、前記認証に成功した場合にのみ、書き込むことを特徴とする請求項 14 に記載の記録媒体装置。

【請求項 23】 前記記録媒体装置は、再生装置に装着され、前記再生装置は、前記情報記憶手段から情報を読み出し、前記耐タンパモジュール手段は、さらに、前記再生装置との間で相互に機器の正当性を認証し、前記認証に成功した場合にのみ、前記再生装置に対して情報の読み出しを許可する認証手段を含むことを特徴とする請求項 14 に記載の記録媒体装置。

【請求項 24】 前記復号部は、複数の復号方式を予め備えており、前記複数の復号方式から選択した 1 個の復号方式を用いて、復号し、ここで、選択した前記復号方式は、前記送信装置で用いられる暗号化方式の逆変換を行うことを特徴とする請求項 14 に記載の記録媒体装置。

【請求項 25】 前記暗号化部は、複数の暗号化方式を予め備えており、前記複数の暗号化方式から選択した 1 個の暗号方式を用いて、暗号化することを特徴とする請求項 14 に記載の記録媒体装置。

【請求項 26】 前記鍵記憶部は、複数の配信復号鍵候補を記憶しており、前記複数の配信復号鍵候補から 1 個の配信復号鍵候補が前記配信復号鍵として選択されており、

前記復号部は、選択された前記配信復号鍵を用いることを特徴とする請求項 1 4 に記載の記録媒体装置。

【請求項 2 7】 前記耐タンパモジュール手段は、ソフトウェア、ハードウェア、又はソフトウェア及びハードウェアの組合せにより、耐タンパ性を実現していることを特徴とする請求項 1 4 に記載の記録媒体装置。

【請求項 2 8】 送信装置からネットワーク及び受信装置を介して送信されて可搬型の記録媒体装置に書き込まれたデジタル著作物を再生する再生装置であって、前記記録媒体装置が前記受信装置に装着され、前記送信装置は、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第 1 暗号化情報を生成し、生成した第 1 暗号化情報をネットワークを介して前記受信装置へ送信し、

前記記録媒体装置は、情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タンパモジュール部とを備え、前記耐タンパモジュール部は、前記受信装置を介して送信された前記第 1 暗号化情報を取得し、配信復号鍵に基づいて前記第 1 暗号化情報を復号して中間情報を生成し、前記記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第 2 暗号化情報を生成し、生成した第 2 暗号化情報を前記情報記憶領域に書き込み、ここで、前記第 2 暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、

前記再生装置は、前記記録媒体装置から前記媒体固有鍵をセキュアに取得する鍵取得手段と、

前記情報記憶領域から前記第 2 暗号化情報を読み出す読出手段と、

取得した前記媒体固有鍵に基づいて、読み出した前記第 2 暗号化を復号して、復号コンテンツを生成する復号手段と、

生成された復号コンテンツを再生する再生手段とを備えることを特徴とする再生装置。

【請求項 2 9】 前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツと第 1 暗号化コンテンツ鍵とを含む前記第 1 暗号化情報を送信し、

前記耐タンパモジュール部は、前記配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶しており、出力された前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を取得し、前記配信復号鍵を用いて、前記第 1 暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第 2 暗

号化コンテンツ鍵を生成し、取得した前記暗号化コンテンツと生成した前記第 2 暗号化コンテンツ鍵とを含む前記第 2 暗号化情報を書き込み、

前記読出手段は、前記暗号化コンテンツと前記第 2 暗号化コンテンツ鍵とを含む前記第 2 暗号化情報を読み出し、

前記復号手段は、取得した前記媒体固有鍵を用いて、読み出した前記第 2 暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成することを特徴とする請求項 2 8 に記載の再生装置。

【請求項 3 0】 前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第 1 暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第 1 暗号化利用条件情報を生成し、前記第 1 暗号化利用条件鍵及び前記第 1 暗号化利用条件情報を、ネットワークを介して、前記受信装置へ送信し、

前記記録媒体装置は、さらに、前記受信装置を介して、前記第 1 暗号化利用条件鍵及び前記第 1 暗号化利用条件情報を取得し、前記配信復号鍵を用いて、前記第 1 暗号化利用条件鍵を復号して中間利用条件鍵を生成し、生成した前記中間利用条件鍵を用いて、前記第 1 暗号化利用条件情報を復号して、中間利用条件情報を生成し、前記媒体固有鍵を用いて、前記中間利用条件情報を暗号化して第 2 暗号化利用条件情報を生成し、生成した第 2 暗号化利用条件情報を前記情報記憶領域に書き込み、

前記読出手段は、さらに、前記情報記憶領域から前記第 2 暗号化利用条件情報を読み出し、

前記復号手段は、さらに、前記媒体固有鍵に基づいて、読み出した前記第 2 暗号化利用条件情報を復号して復号利用条件情報を生成し、

前記再生手段は、さらに、生成された復号利用条件情報に基づいて復号コンテンツの再生の可否を判断し、再生可と判断される場合にのみ、前記生成された復号コンテンツを再生することを特徴とする請求項 2 9 に記載の再生装置。

【請求項 3 1】 前記利用条件情報は、前記復号コンテンツの再生回数を制限する情報、前記復号コンテンツの再生期間を制限する情報、又は前記復号コンテンツの再生累積時間を制限する情報を含み、

前記再生手段は、再生回数を制限する情報、再生期間を制限する情報、又は再生累積時間を制御する情報に基づいて復号コンテンツの再生の可否を判断することを特徴とする請求項 3 0 に記載の再生装置。

【請求項 3 2】 前記再生装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証する認証手段

を含み、
前記鍵取得手段は、前記認証に成功した場合にのみ、取得し、
前記読出手段は、前記認証に成功した場合にのみ、読み出すことを特徴とする請求項 29 に記載の再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル著作物の著作権保護を実現する技術に関し、特に、デジタル著作物の再生及び記録における著作権保護技術に関する。

【0002】

【従来の技術】近年、デジタル化された文書、音楽、映像、プログラムなどのデジタル著作物がインターネットなどのネットワークを経由して流通し、利用者は、様々なデジタル著作物を簡単にネットワークを経由して取り出し、記録媒体に記録し、再生することができるようになってきている。

【0003】しかしながら、このように簡単にデジタル著作物を複製できるという利点はあるものの、著作権の著作権が侵害されやすいという問題点がある。その対策として、例えば従来の電子音楽配信システムは、次のようにしている。

(1) コンテンツ提供サーバは、暗号化コンテンツ、そのコンテンツの暗号化に用いるタイトル鍵、及びそのコンテンツの利用条件データを記憶している。ここで、暗号化コンテンツは、音楽などのコンテンツが、コンテンツ毎に固有の前記タイトル鍵で暗号化されたものである。また、ユーザからの要求に応じて送信されるコンテンツに対応するタイトル鍵及び利用条件データを、そのユーザに固有のユーザ固有鍵で暗号化して、暗号化タイトル鍵及び暗号化利用条件データを生成する。

【0004】利用者が有するパソコンは、利用者の指示により、ネットワークを介して接続されたコンテンツ提供サーバから暗号化コンテンツ、暗号化タイトル鍵及び暗号化利用条件データを取得して、記憶する。

(2) パソコンは、あらかじめユーザ固有鍵を記憶している。また、コンテンツを記録するための記録媒体が、利用者によりパソコンに装着される。記録媒体は、あらかじめ記録媒体毎に固有の媒体固有鍵を記憶している。

【0005】パソコンは、利用者の指示により、記憶している暗号化タイトル鍵及び暗号化利用条件データを、ユーザ固有鍵を用いて復号して、一時的に復号タイトル鍵及び復号利用条件データを生成する。次に、パソコンは、装着されている記録媒体から媒体固有鍵をセキュアに読み出し、読み出した媒体固有鍵を用いて復号タイトル鍵及び復号利用条件データを暗号化して、再暗号化タイトル鍵と再暗号化利用条件データを生成し、暗号化コンテンツ、再暗号化タイトル鍵及び再暗号化利用条件データを記録媒体に記録する。記録媒体への記録が完了すると、パソコンは、一時的に生成した復号タイトル鍵及

び復号利用条件データを削除する。

【0006】(3) ユーザは、パソコンから記録媒体を抜き出し、抜き出した記録媒体を再生装置に装着する。再生装置は、記録媒体から媒体固有鍵をセキュアに読み出し、暗号化コンテンツ、再暗号化タイトル鍵及び再暗号化利用条件データを読み出す。次に、再生装置は、読み出した媒体固有鍵を用いて再暗号化タイトル鍵及び再暗号化利用条件データを復号して、タイトル鍵及び利用条件データを生成する。次に、再生装置は、生成したタイトル鍵を用いて暗号化コンテンツを復号してコンテンツを生成し、生成した利用条件データによって許諾された範囲内で、生成したコンテンツを、再生する。

【0007】

【発明が解決しようとする課題】しかしこのようなシステムでは、パソコン上で暗号化タイトル鍵を一旦復号し、次に再度暗号化する（以下では、暗号変換と称する）ので、パソコン上に一時的に復号されたタイトル鍵が生成されて記憶される。このため、悪意のある利用者は、パソコン上に一時的に生成されたタイトル鍵を知ることが技術的に可能であり、こうして不正に取得したタイトル鍵を用いて、暗号化コンテンツを不正に復号することができる（以下、このような行為をハッキングと呼ぶ）という問題がある。

【0008】このような問題点を解決するために、従来、パソコン内のコンピュータプログラムに、本来必要な命令や分岐命令をあらかじめ含ませておいて、ハッキングが困難になるようにしている。しかしながら、プログラムの増大を招き、また速度性能が低下するという問題点がある。本発明は、上述した問題点を解決するために、プログラムの量が増加することなく、また速度性能が低下することなく、上述のようなハッキングを困難にするデジタル著作物保護システム、記録媒体装置、送信装置及び再生装置を提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するために、本発明は、送信装置から送信されたデジタル著作物を、受信装置を介して、可搬型の記録媒体装置に書き込み、再生装置により再生するデジタル著作物保護システムであって、前記デジタル著作物保護システムは、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第 1 暗号化情報を生成し、生成した第 1 暗号化情報をネットワークを介して送信する前記送信装置を含み、ここで、前記記録媒体装置が前記受信装置に装着され、前記デジタル著作物保護システムは、さらに、ネットワークを介して前記第 1 暗号化情報を受信し、受信した前記第 1 暗号化情報を前記記録媒体装置へ出力する受信装置と、情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タンパモジュール部とを備える前記記録媒体装置とを含み、前記耐タンパモジュール部は、出力された前記第 1 暗号化情報を取得し、配信復号鍵に

基づいて前記第 1 暗号化情報を復号して中間情報を生成し、前記記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第 2 暗号化情報を生成し、生成した第 2 暗号化情報を前記情報記憶領域に書き込み、ここで、前記第 2 暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、前記デジタル著作物保護システムは、さらに、前記情報記憶領域から前記第 2 暗号化情報を読み出し、前記媒体固有鍵をセキュアに読み出し、前記媒体固有鍵に基づいて前記第 2 暗号化情報を復号して復号コンテンツを生成し、生成した復号コンテンツを再生する前記再生装置を含むことを特徴とする。

【0010】ここで、前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる前記配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した前記配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツと第 1 暗号化コンテンツ鍵とを含む前記第 1 暗号化情報を送信し、前記受信装置は、前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を受信し、受信した前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を出力し、前記耐タンパモジュール部は、配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶しており、出力された前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を取得し、前記配信復号鍵を用いて、前記第 1 暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第 2 暗号化コンテンツ鍵を生成し、取得した前記暗号化コンテンツと生成した前記第 2 暗号化コンテンツ鍵とを含む前記第 2 暗号化情報を書き込み、前記再生装置は、前記記録媒体装置から前記媒体固有鍵をセキュアに取得し、前記情報記憶領域から、前記暗号化コンテンツと前記第 2 暗号化コンテンツ鍵とを含む前記第 2 暗号化情報を読み出し、取得した前記媒体固有鍵を用いて、前記第 2 暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成するように構成してもよい。

【0011】また、本発明は、デジタル著作物を送信する送信装置と、ネットワークを介して受信した前記デジタル著作物を可搬型の記録媒体装置に記録する受信装置と、前記記録媒体装置に記録された前記デジタル著作物を再生する再生装置と、前記記録媒体装置とから構成されるデジタル著作物保護システムであって、前記送信装置は、デジタル著作物である原コンテンツと当該原コンテンツに固有の原コンテンツ鍵を予め記憶している記憶

手段と、デジタル著作物の配信のために用いられる配信暗号鍵を取得する配信暗号鍵取得手段と、前記原コンテンツ鍵を用いて、前記原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成する暗号化手段と、前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を、ネットワークを介して、送信する送信手段とを含み、ここで、前記記録媒体装置が前記受信装置に装着され、前記受信装置は、ネットワークを介して前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を受信する受信手段と、受信した前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を出力する出力手段とを含み、前記記録媒体装置は、情報を記憶するための領域を備えている情報記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを含み、前記耐タンパモジュール手段は、配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶している鍵記憶部と、出力された前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を取得する取得部と、前記配信復号鍵を用いて、前記第 1 暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成する復号部と、前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第 2 暗号化コンテンツ鍵を生成する暗号化部と、取得した前記暗号化コンテンツ及び生成した前記第 2 暗号化コンテンツ鍵を前記情報記憶手段に書き込む書込部とを含み、ここで、前記暗号化コンテンツ及び前記第 2 暗号化コンテンツ鍵が書き込まれた前記記録媒体装置が前記再生装置に装着され、前記再生装置は、前記鍵記憶部から前記媒体固有鍵をセキュアに取得する鍵取得手段と、前記情報記憶手段から前記暗号化コンテンツと前記第 2 暗号化コンテンツ鍵とを読み出す読出手段と、取得した前記媒体固有鍵を用いて、読み出した前記第 2 暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成するコンテンツ鍵復号手段と、生成された前記復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成するコンテンツ復号手段と、生成された復号コンテンツを再生する再生手段とを備えることを特徴とする。

【0012】また、本発明は、デジタル著作物をネットワークを介して送信する送信装置であって、前記デジタル著作物は、受信装置を介して、可搬型の記録媒体装置に書き込まれ、前記送信装置は、デジタル著作物である原コンテンツと当該原コンテンツに固有の原コンテンツ鍵を予め記憶している記憶手段と、デジタル著作物の配信のために用いられる配信暗号鍵を取得する配信暗号鍵取得手段と、前記原コンテンツ鍵を用いて、前記原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成する暗号化手段と、前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵

を、ネットワークを介して、送信する送信手段とを備えることを特徴とする。

【0013】ここで、前記記憶手段は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記暗号化手段は、さらに、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第1暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第1暗号化利用条件情報を生成し、前記送信手段は、さらに、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を、ネットワークを介して、送信するように構成してもよい。

【0014】ここで、前記配信暗号鍵取得手段は、公開鍵生成アルゴリズムを用いて生成された公開鍵である前記配信暗号鍵を取得し、前記暗号化手段は、公開鍵である配信暗号鍵を用いて、公開鍵暗号アルゴリズムにより、暗号化するように構成してもよい。ここで、前記送信装置は、さらに、無効の配信暗号鍵を記録するための領域を備えるリポークリスト手段と、公開鍵である前記配信暗号鍵の生成において基にされた配信復号鍵が暴露された場合に、前記配信暗号鍵を前記リポークリスト手段に書き込む登録手段とを含み、ここで、前記送信装置は、新たにデジタル著作物であるコンテンツを送信し、前記配信鍵取得手段は、新たに配信暗号鍵を取得し、取得した配信暗号鍵がリポークリスト手段に書き込まれているか否かを判断し、書き込まれていると判断する場合には、前記暗号化手段に対して暗号化を禁止し、前記送信手段に対して送信を禁止するように構成してもよい。

【0015】ここで、前記記憶手段は、さらに、前記デジタル著作物の利用条件を示す利用条件情報を記憶しており、前記送信手段は、さらに、前記記憶手段から前記利用条件情報を読み出し、読み出した前記利用条件情報にハッシュアルゴリズムを施してハッシュ値を生成し、生成した前記ハッシュ値と読み出した利用条件情報を、セキュアにネットワークを介して送信するように構成してもよい。

【0016】ここで、前記送信装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証する認証手段を含み、前記配信暗号鍵取得手段は、前記認証に成功した場合にのみ、前記配信暗号鍵を前記記録媒体装置から取得し、前記暗号化手段は、前記認証に成功した場合にのみ、暗号化し、前記送信手段は、前記認証に成功した場合にのみ、送信するように構成してもよい。

【0017】ここで、前記送信装置は、さらに、前記記録媒体装置が備える耐タンパモジュール部を更新するための更新情報を予め記憶している更新情報記憶手段と、前記更新情報記憶手段から前記更新情報を読み出し、読み出した前記更新情報を、ネットワーク及び受信装置を介して、前記記録媒体装置へ送信する更新情報送信手段とを含むように構成してもよい。

【0018】ここで、前記送信装置は、さらに、前記更新情報記憶手段から前記更新情報を読み出し、読み出した更新情報にハッシュアルゴリズムを施してハッシュ値を生成し、生成したハッシュ値を、ネットワーク及び受信装置を介して、前記記録媒体装置へセキュアに送信するハッシュ手段を含むように構成してもよい。ここで、前記更新情報記憶手段が記憶している更新情報は、前記耐タンパモジュール部が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含み、前記更新情報送信手段は、前記耐タンパモジュール部が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含む前記更新情報を読み出し、読み出した前記更新情報を送信するように構成してもよい。

【0019】また、本発明は、送信装置から送信されたデジタル著作物を、受信装置を介して、記録する可搬型の記録媒体装置であって、前記記録媒体装置が前記受信装置に装着され、前記送信装置は、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報を、ネットワークを介して、前記受信装置へ送信し、前記記録媒体装置は、情報を記憶するための領域を備える情報記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備え、前記耐タンパモジュール手段は、配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶している鍵記憶部と、前記受信装置を介して、送信された前記第1暗号化情報を取得する取得部と、前記配信復号鍵に基づいて前記第1暗号化情報を復号して中間情報を生成する復号部と、前記媒体固有鍵に基づいて前記中間情報を暗号化して第2暗号化情報を生成する暗号化部と、生成した第2暗号化情報を前記情報記憶手段に書き込む書込部とを備えることを特徴とする。

【0020】ここで、前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第1暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ及び第1暗号化コンテンツ鍵を含む前記第1暗号化情報を送信し、前記取得部は、出力された前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を含む前記第1暗号化情報を取得し、前記復号部は、前記配信復号鍵を用いて、前記第1暗号化情報に含まれる前記第1暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記第1暗号化情報に含まれる前記暗号化コンテンツ及び生成した前記中間コンテンツ鍵を含む前記中間情報を生成し、前記暗号化部は、前記媒体固有鍵を用いて、前記中間情報に含まれる前記中間コンテンツ鍵

を暗号化して第2暗号化コンテンツ鍵を生成し、前記中間情報に含まれる前記暗号化コンテンツ及び生成した前記第2暗号化コンテンツ鍵を含む前記第2暗号化情報を生成し、前記書込部は、前記暗号化コンテンツ及び前記第2暗号化コンテンツ鍵を含む前記第2暗号化情報を書き込むように構成してもよい。

【0021】ここで、前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第1暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第1暗号化利用条件情報を生成し、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を、ネットワークを介して、前記受信装置へ送信し、前記取得部は、さらに、前記受信装置を介して、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を取得し、前記復号部は、さらに、前記配信復号鍵を用いて、前記第1暗号化利用条件鍵を復号して中間利用条件鍵を生成し、生成した前記中間利用条件鍵を用いて、前記第1暗号化利用条件情報を復号して、中間利用条件情報を生成し、前記暗号化部は、さらに、前記媒体固有鍵を用いて、前記中間利用条件情報を暗号化して第2暗号化利用条件情報を生成し、前記書込部は、さらに、生成した第2暗号化利用条件情報を前記情報記憶手段に書き込むように構成してもよい。

【0022】ここで、前記送信装置は、さらに、秘密鍵である配信用復号鍵を基にして公開鍵生成アルゴリズムを用いて生成された公開鍵である前記配信暗号鍵を取得し、公開鍵である配信暗号鍵を用いて、公開鍵暗号アルゴリズムにより、暗号化し、前記復号部は、公開鍵復号アルゴリズムにより、前記配信用復号鍵を用いて復号するように構成してもよい。

【0023】ここで、前記耐タンパモジュール手段は、さらに、前記復号部により生成された配信データ形式である前記中間情報を変換して、記録データ形式の記録中間情報を生成する変換部を含み、前記暗号化部は、前記中間情報に代えて、前記記録中間情報を暗号化するように構成してもよい。ここで、前記送信装置は、前記記録媒体装置が備える前記耐タンパモジュール手段を更新するための更新情報を予め記憶しており、前記更新情報を読み出し、読み出した前記更新情報を、ネットワーク及び受信装置を介して、前記記録媒体装置へ送信し、前記耐タンパモジュール手段は、マイクロプロセッサとコンピュータプログラムを記録している半導体メモリを含み、前記コンピュータプログラムに従って、前記マイクロプロセッサが動作することにより、前記耐タンパモジュール手段に含まれる構成要素が動作し、前記取得部は、前記受信装置を介して、前記更新情報を取得し、前記耐タンパモジュール手段は、さらに、取得した前記更新情報を用いて、前記コンピュータプログラムを更新

し、これにより、前記耐タンパモジュール手段に含まれる構成要素が更新される更新部を含むように構成してもよい。

【0024】ここで、前記送信装置は、さらに、前記更新情報を読み出し、読み出した更新情報にハッシュアルゴリズムを施して第1ハッシュ値を生成し、生成した第1ハッシュ値を、ネットワーク及び受信装置を介して、前記記録媒体装置へセキュアに送信し、前記耐タンパモジュール手段は、さらに、取得した前記更新情報に前記ハッシュアルゴリズムを施して第2ハッシュ値を生成するハッシュ部と、取得した前記第1ハッシュ値と生成した前記第2ハッシュ値とが一致するか否かを判断する比較判断部とを含み、前記更新部は、前記比較判断部により一致すると判断された場合にのみ、更新するように構成してもよい。

【0025】ここで、前記送信装置が記憶している更新情報は、前記耐タンパモジュール手段が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含み、前記前記更新情報を送信し、前記取得部は、暗号化方式、復号方式、又はデータ変換方式を更新するための前記更新情報を前記受信装置を介して取得し、前記更新部は、取得した前記更新情報を用いて、前記コンピュータプログラムを更新し、これにより、前記耐タンパモジュール手段に含まれる暗号化部、復号部、又は変換部が更新されるように構成してもよい。

【0026】ここで、前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報を記憶しており、前記利用条件情報を読み出し、読み出した前記利用条件情報にハッシュアルゴリズムを施して第1ハッシュ値を生成し、生成した前記第1ハッシュ値と読み出した利用条件情報を、ネットワークを介してセキュアに送信し、前記取得部は、さらに、前記受信装置を介して、送信された前記第1ハッシュ値と前記利用条件情報とを取得し、前記耐タンパモジュール手段は、さらに、取得した前記利用条件情報に前記ハッシュアルゴリズムを施して第2ハッシュ値を生成するハッシュ部と、取得した前記第1ハッシュ値と生成した前記第2ハッシュ値とが一致するか否かを判断する比較判断部とを含み、前記暗号化部は、前記比較判断部により一致すると判断された場合にのみ、暗号化し、前記書込部は、前記比較判断部により一致すると判断された場合にのみ、書き込むように構成してもよい。

【0027】ここで、前記送信装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証し、前記認証に成功した場合にのみ、前記配信暗号鍵を前記記録媒体装置から取得し、暗号化し、送信し、前記耐タンパモジュール手段は、さらに、前記送信装置との間で相互に機器の正当性を認証する認証手段を含み、前記取得部は、前記認証に成功した場合にのみ、取得し、前記復号

部は、前記認証に成功した場合にのみ、復号し、前記暗号化部は、前記認証に成功した場合にのみ、暗号化し、前記書込部は、前記認証に成功した場合にのみ、書き込むように構成してもよい。

【0028】ここで、前記記録媒体装置は、再生装置に装着され、前記再生装置は、前記情報記憶手段から情報を読み出し、前記耐タンパモジュール手段は、さらに、前記再生装置との間で相互に機器の正当性を認証し、前記認証に成功した場合にのみ、前記再生装置に対して情報の読み出しを許可する認証手段を含むように構成してもよい。

【0029】ここで、前記復号部は、複数の復号方式を予め備えており、前記複数の復号方式から選択した1個の復号方式を用いて、復号し、ここで、選択した前記復号方式は、前記送信装置で用いられる暗号化方式の逆変換を行うように構成してもよい。また、前記暗号化部は、複数の暗号化方式を予め備えており、前記複数の暗号化方式から選択した1個の暗号方式を用いて、暗号化するように構成してもよい。

【0030】ここで、前記鍵記憶部は、複数の配信復号鍵候補を記憶しており、前記複数の配信復号鍵候補から1個の配信復号鍵候補が前記配信復号鍵として選択されており、前記復号部は、選択された前記配信復号鍵を用いるように構成してもよい。ここで、前記耐タンパモジュール手段は、ソフトウェア、ハードウェア、又はソフトウェア及びハードウェアの組合せにより、耐タンパ性を実現しているように構成してもよい。

【0031】また、本発明は、送信装置からネットワーク及び受信装置を介して送信されて可搬型の記録媒体装置に書き込まれたデジタル著作物を再生する再生装置であって、前記記録媒体装置が前記受信装置に装着され、前記送信装置は、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報をネットワークを介して前記受信装置へ送信し、前記記録媒体装置は、情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タンパモジュール部とを備え、前記耐タンパモジュール部は、前記受信装置を介して送信された前記第1暗号化情報を取得し、配信復号鍵に基づいて前記第1暗号化情報を復号して中間情報を生成し、前記記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第2暗号化情報を生成し、生成した第2暗号化情報を前記情報記憶領域に書き込み、ここで、前記第2暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、前記再生装置は、前記記録媒体装置から前記媒体固有鍵をセキュアに取得する鍵取得手段と、前記情報記憶領域から前記第2暗号化情報を読み出す読出手段と、取得した前記媒体固有鍵に基づいて、読み出した前記第2暗号化を復号して、復号コンテンツを生成する復号手段と、生成された復号コンテンツを再生する再生手段とを

備えることを特徴とする。

【0032】ここで、前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第1暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツと第1暗号化コンテンツ鍵とを含む前記第1暗号化情報を送信し、前記耐タンパモジュール部は、前記配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶しており、出力された前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を含む前記第1暗号化情報を取得し、前記配信復号鍵を用いて、前記第1暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第2暗号化コンテンツ鍵を生成し、取得した前記暗号化コンテンツと生成した前記第2暗号化コンテンツ鍵とを含む前記第2暗号化情報を書き込み、前記読出手段は、前記暗号化コンテンツと前記第2暗号化コンテンツ鍵とを含む前記第2暗号化情報を読み出し、前記復号手段は、取得した前記媒体固有鍵を用いて、読み出した前記第2暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成するように構成してもよい。

【0033】ここで、前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第1暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第1暗号化利用条件情報を生成し、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を、ネットワークを介して、前記受信装置へ送信し、前記記録媒体装置は、さらに、前記受信装置を介して、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を取得し、前記配信復号鍵を用いて、前記第1暗号化利用条件鍵を復号して中間利用条件鍵を生成し、生成した前記中間利用条件鍵を用いて、前記第1暗号化利用条件情報を復号して、中間利用条件情報を生成し、前記媒体固有鍵を用いて、前記中間利用条件情報を暗号化して第2暗号化利用条件情報を生成し、生成した第2暗号化利用条件情報を前記情報記憶領域に書き込み、前記読出手段は、さらに、前記情報記憶領域から前記第2暗号化利用条件情報を読み出し、前記復号手段は、さらに、前記媒体固有鍵に基づいて、読み出した前記第2暗号化利用条件情報を復号して復号利用条件情報を生成し、前記再生手段は、さらに、生成された復号利用条件情報に基づいて復号コンテンツの再生の可否を判断し、再生可と判断される場合にのみ、前記生

成された復号コンテンツを再生するように構成してもよい。

【0034】ここで、前記利用条件情報は、前記復号コンテンツの再生回数を制限する情報、前記復号コンテンツの再生期間を制限する情報、又は前記復号コンテンツの再生累積時間を制限する情報を含み、前記再生手段は、再生回数を制限する情報、再生期間を制限する情報、又は再生累積時間を制御する情報に基づいて復号コンテンツの再生の可否を判断するように構成してもよい。

【0035】ここで、前記再生装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証する認証手段を含み、前記鍵取得手段は、前記認証に成功した場合にのみ、取得し、前記読出手段は、前記認証に成功した場合にのみ、読み出すように構成してもよい。

【0036】

【発明の実施の形態】 1. 実施の形態 1

本発明に係る実施の形態としてのデジタル著作物保護システム 100 について説明する。デジタル著作物保護システム 100 は、図 1 に示すように、コンテンツ配信用サーバ装置 200、パーソナルコンピュータ (PC) 300、可搬型のメモリカード 400 及び、ヘッドホンステレオ 500 から構成されており、PC 300 は、インターネット 10 を介してコンテンツ配信用サーバ装置 200 に接続されている。

【0037】利用者は、メモリカード 400 を PC 300 に装着する。PC 300 は、利用者の指示により、コンテンツ配信用サーバ装置 200 から暗号化コンテンツを取得し、取得した暗号化コンテンツをメモリカード 400 に書き込む。次に、利用者は、PC 300 からメモリカード 400 を抜き出し、抜き出したメモリカード 400 をヘッドホンステレオ 500 に装着する。ヘッドホンステレオ 500 は、メモリカード 400 に記録されている暗号化コンテンツを復号してコンテンツを生成し、生成したコンテンツを再生してヘッドホン 700 へ出力する。

【0038】このようにして利用者は、再生されたコンテンツを楽しむことができる。

1. 1 コンテンツ配信用サーバ装置 200 の構成

コンテンツ配信用サーバ装置 200 は、図 2 に示すように、コンテンツ格納部 201、配信データ格納部 202、第 1 認証部 211、配信公開鍵取得部 212、楕円暗号化部 214、DES 暗号化部 215 及び DES 暗号化部 250 から構成されている。

【0039】コンテンツ配信用サーバ装置 200 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、LAN 接続ユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記 RAM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶

されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、コンテンツ配信用サーバ装置 200 は、その機能を達成する。

【0040】(1) コンテンツ格納部 201

コンテンツ格納部 201 は、具体的には、ハードディスクユニットから構成され、あらかじめ音楽、映画、電子書籍、ゲームプログラムなどのデジタル著作物であるコンテンツ 600 を記憶している。

(2) 配信データ格納部 202

10 配信データ格納部 202 は、具体的には、ハードディスクユニットから構成され、図 6 に示すように、あらかじめタイトル鍵、利用条件鍵及び利用条件データをこの順序で記憶しており、タイトル鍵、利用条件鍵及び利用条件データは、コンテンツ格納部 201 が記憶しているコンテンツ 600 に対応している。

【0041】タイトル鍵は、コンテンツ毎にランダムに生成された乱数からなり、56 ビット長である。利用条件鍵は、利用条件毎にランダムに生成された乱数からなり、56 ビット長である。利用条件データは、再生回数情報、再生期間情報及び再生累積時間情報から構成される。

【0042】再生回数情報は、16 ビット長であり、利用者に対して、当該利用条件データに対応して記憶されているコンテンツを再生することができる回数の合計値を制限するものである。例えば、再生回数情報が、「10」である場合に、利用者に対して、当該コンテンツを最大 10 回まで再生することが許可される。また、再生回数情報として、「FFFF」(16 進数) が指定された場合には、無制限に再生が可能であることを示すものとする。

【0043】再生期間情報は、64 ビット長であり、利用者に対して、当該利用条件データに対応して記憶されているコンテンツを再生することができる期間を制限するものであり、再生期間の開始日時を示す再生許可開始日時と、再生期間の終了日時を示す再生許可終了日時とから構成される。利用者に対して、再生許可開始日時から再生許可終了日時までの期間内においてのみ、当該コンテンツの再生が許可される。この期間内であれば、利用者は、当該コンテンツを何回でも再生することができる。

【0044】ここで、再生期間情報及び再生回数情報の両方が指定されている場合には、許可されている期間が終了するか、又は再生回数まで再生した後は、コンテンツを再生することはできないものとする。再生累積時間情報は、利用者に対して、当該利用条件データに対応して記憶されているコンテンツを再生することができる時間の累積値を制限するものである。例えば、再生累積時間情報が、「10 時間」である場合に、利用者に対して、当該コンテンツの再生時間の累積値が 10 時間以内であれば、当該コンテンツの再生が許可される。10 時

間を超えると、再生が禁止される。

【0045】なお、利用条件データは、再生回数情報、再生期間情報及び再生累積時間情報から構成されるとしているが、利用条件データは、再生回数情報、再生期間情報及び再生累積時間情報の全て、いずれか2個の組合せ、又はいずれか1個から構成されるとしてもよい。

(3) 第1認証部211

第1認証部211は、インターネット10及びPC300を介して、メモリカード400が有する第1認証部411（後述する）との間で、チャレンジレスポンス型の相互の機器認証を行う。具体的には、第1認証部211は、第1認証部411の認証を行う。次に、第1認証部211は、第1認証部411による認証を受ける。両方の認証が成功した場合にのみ、相互の機器認証が成功したものと見做される。なお、チャレンジレスポンス型の機器認証については、公知であるので、説明を省略する。

【0046】両者の認証が成功した場合に、第1認証部211は、認証の成功を示す認証成功情報を、配信公開鍵取得部212、楕円暗号化部214及びDES暗号化部215へ出力する。認証が失敗した場合に、第1認証部211は、以降の処理を中止する。従って、コンテンツ配信サーバ装置200が記憶しているコンテンツがメモリカード400へ出力されることはない。

【0047】(4) 配信公開鍵取得部212

配信公開鍵取得部212は、第1認証部211から認証成功情報を受け取る。認証成功情報を受け取ると、配信公開鍵取得部212は、インターネット10及びPC300を介して、メモリカード400が有する配信公開鍵格納部412（後述する）から配信公開鍵をセキュアに受け取り、受け取った配信公開鍵を楕円暗号化部214へ出力する。

【0048】(5) 楕円暗号化部214

楕円暗号化部214は、第1認証部211から認証成功情報を受け取る。認証成功情報を受け取ると、楕円暗号化部214は、配信公開鍵取得部212から配信公開鍵を受け取り、配信データ格納部202からタイトル鍵及び利用条件鍵を読み出す。次に、楕円暗号化部214は、受け取った前記配信公開鍵を鍵として用いて、タイトル鍵と利用条件鍵とを結合した結合情報に、楕円暗号方式による暗号アルゴリズムE1を施して暗号化結合情報を生成し、生成した暗号化結合情報をインターネット10及びPC300を介して、メモリカード400が有する楕円復号部414（後述する）へ出力する。

【0049】なお、楕円暗号についてはDouglas R. Stinson著「暗号理論の基礎」（共立出版株式会社、1996年）に詳細に説明されている。また、図2において、各ブロックは、接続線により他のブロックと接続されている。ここで、各接続線は、信号や情報が伝達される経路を示している。楕円暗号化部21

4を示すブロックに接続している複数の接続線のうち、接続線上に鍵マークが付されているものは、楕円暗号化部214へ鍵としての情報が伝達される経路を示している。DES暗号化部215を示すブロックについても同様である。また、他の図面についても同様である。

【0050】(6) DES暗号化部215

DES暗号化部215は、第1認証部211から認証成功情報を受け取る。認証成功情報を受け取ると、DES暗号化部215は、配信データ格納部202から利用条件鍵及び利用条件データを読み出す。次に、DES暗号化部215は、読み出した前記利用条件鍵を鍵として用いて、読み出した前記利用条件データに、DES（Data Encryption Standard）による暗号アルゴリズムE2を施して暗号化利用条件データを生成し、生成した暗号化利用条件データをインターネット10及びPC300を介して、メモリカード400が有するDES復号部415（後述する）へ出力する。

【0051】(7) DES暗号化部250

DES暗号化部250は、配信データ格納部202からタイトル鍵を読み出し、コンテンツ格納部201からコンテンツ600を読み出す。次に、DES暗号化部250は、読み出した前記タイトル鍵を鍵として用いて、読み出した前記コンテンツに、DESによる暗号アルゴリズムE3を施して暗号化コンテンツを生成し、生成した暗号化コンテンツをインターネット10及びPC300を介して、メモリカード400が有する情報記憶部430（後述する）内の第1記憶領域432（後述する）へ書き込む。

【0052】1.2 PC300の構成

PC300は、図4に示すように、マイクロプロセッサ301、ROM、RAM、ハードディスクユニットなどのメモリ部302、キーボード、マウスなどの入力部303、ディスプレイユニットなどの表示部304、インターネット10を介して外部と通信を行うための通信部305、メモリカード400との間の接続を行うメモリカード接続部306などから構成されるコンピュータシステムである。メモリ部302には、コンピュータプログラムが記憶されている。前記マイクロプロセッサ301が、前記コンピュータプログラムに従って動作することにより、PC300は、その機能を達成する。

【0053】1.3 メモリカード400の構成

メモリカード400は、図3に示すように、外部から読み書きできない耐タンパモジュール部410と情報記憶部430とから構成されている。耐タンパモジュール部410は、第1認証部411、配信公開鍵格納部412、配信秘密鍵格納部413、楕円復号部414、DES復号部415、変換部416、第2認証部417、記録媒体鍵格納部418、DES暗号化部419、配信データ格納部423及び記録データ格納部422から構成され、情報記憶部430は、第1記憶領域432と第2

記憶領域 431 とを含んで構成されている。ここで、耐タンパモジュール部 410 は、具体的には、耐タンパハードウェアにより構成されているものとする。なお、耐タンパモジュール部 410 は、耐タンパソフトウェア、又は耐タンパハードウェア及び耐タンパソフトウェアの組み合わせで構成されているとしてもよい。

【0054】また、耐タンパモジュール部 410 は、具体的には、マイクロプロセッサ、ROM、RAM などから構成され、前記 RAM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、耐タンパモジュール部 410 装置は、その機能を達成する。

【0055】(1) 配信秘密鍵格納部 413

配信秘密鍵格納部 413 は、あらかじめ配信秘密鍵を記憶している。配信秘密鍵は、160 ビット長のデータである。

(2) 配信公開鍵格納部 412

配信公開鍵格納部 412 は、あらかじめ配信公開鍵を記憶している。配信公開鍵は、320 ビット長のデータである。配信公開鍵は、配信秘密鍵格納部 413 に格納されている配信秘密鍵を基にして、楕円暗号方式による公開鍵生成アルゴリズムを用いて生成されたものである。

【0056】配信公開鍵格納部 412 は、第 1 認証部 411 から認証成功情報を受け取る。認証成功情報を受け取ると、配信公開鍵格納部 412 は、コンテンツ配信サーバ装置 200 が有する配信公開鍵取得部 212 からの要求に応じて、内部に記憶している配信公開鍵を読み出し、読み出した配信公開鍵を PC300 及びインターネット 10 を介して、コンテンツ配信サーバ装置 200 へ出力する。

【0057】(3) 記録媒体鍵格納部 418

記録媒体鍵格納部 418 は、あらかじめメモリカード 400 に固有の記録媒体鍵を記憶している。記録媒体鍵は、56 ビット長のデータである。

(4) 配信データ格納部 423

配信データ格納部 423 は、タイトル鍵、利用条件鍵及び利用条件データを記憶するための領域を備えている。

【0058】(5) 記録データ格納部 422

記録データ格納部 422 は、タイトル鍵及び利用条件データを記憶するための領域を備えている。記録データ格納部 422 に記録されるタイトル鍵及び利用条件データのデータ形式は、図 7 に示すとおりであり、タイトル鍵及び利用条件データがこの順序で並べられている。

【0059】(6) 第 1 記憶領域 432

第 1 記憶領域 432 は、暗号化コンテンツを記憶するための領域を備えている。第 1 記憶領域 432 は、コンテンツ配信サーバ装置 200 から、インターネット 10 及び PC300 を介して、暗号化コンテンツを受け取り、受け取った暗号化コンテンツを記憶する。

【0060】(7) 第 2 記憶領域 431

第 2 記憶領域 431 は、再暗号化タイトル鍵及び再暗号化利用条件データを記憶するための領域を備えている。第 2 記憶領域 431 は、第 2 認証部 417 から認証の成功を示す認証成功情報を受け取る。認証成功情報を受け取ると、第 2 記憶領域 431 は、再暗号化タイトル鍵及び再暗号化利用条件データを読み出して、出力する。

【0061】(8) 第 1 認証部 411

第 1 認証部 411 は、PC300 及びインターネット 10 を介して、コンテンツ配信サーバ装置 200 が有する第 1 認証部 211 との間で、チャレンジャーレスポンス型の相互の機器認証を行う。具体的には、第 1 認証部 411 は、第 1 認証部 211 による認証を受ける。次に、第 1 認証部 411 は、第 1 認証部 211 を認証する。両方の認証が成功した場合にのみ、相互の機器認証が成功したものと見做される。なお、チャレンジャーレスポンス型の機器認証については、公知であるので、説明を省略する。

【0062】両者の認証が成功した場合に、第 1 認証部 411 は、認証の成功を示す認証成功情報を、配信公開鍵格納部 412 へ出力する。認証が失敗した場合に、第 1 認証部 411 は、以降の処理を中止する。従って、コンテンツ配信サーバ装置 200 によりメモリカード 400 へ各種情報が書き込まれることはない。

【0063】(9) 楕円復号部 414

楕円復号部 414 は、コンテンツ配信サーバ装置 200 から、インターネット 10 及び PC300 を介して、暗号化結合情報を受け取る。暗号化結合情報を受け取ると、楕円復号部 414 は、配信秘密鍵格納部 413 から配信秘密鍵を読み出し、読み出した配信秘密鍵を鍵として用いて、受け取った暗号化結合情報に楕円暗号方式による復号アルゴリズム D1 を施して、タイトル鍵及び利用条件鍵を生成し、生成したタイトル鍵及び利用条件鍵を配信データ格納部 423 へ書き込む。

【0064】ここで、復号アルゴリズム D1 は、暗号アルゴリズム E1 の逆変換を行うアルゴリズムである。

(10) DES 復号部

DES 復号部は、コンテンツ配信サーバ装置 200 から、インターネット 10 及び PC300 を介して、暗号化利用条件データを受け取る。暗号化利用条件データを受け取ると、DES 復号部は、配信データ格納部 423 から利用条件鍵を読み出す。次に、読み出した利用条件鍵を鍵として用いて、受け取った暗号化利用条件データに、DES による復号アルゴリズム D2 を施して利用条件データを生成し、生成した利用条件データを配信データ格納部 423 へ書き込む。

【0065】ここで、復号アルゴリズム D2 は、暗号アルゴリズム E2 の逆変換を行うアルゴリズムである。

(11) 変換部 416

変換部 416 は、配信データ格納部 423 からタイトル

鍵及び利用条件データを読み出し、読み出したタイトル鍵及び利用条件データをこの順序で、記録データ格納部 422 へ書き込む。

【0066】(12) 第2認証部 417

第2認証部 417 は、ヘッドホンステレオ 500 が有する第1認証部 517 との間で、チャレンジャーレスポンス型の相互の機器認証を行う。具体的には、第2認証部 417 は、第2認証部 517 による認証を受ける。次に、第2認証部 417 は、第2認証部 517 を認証する。両方の認証が成功した場合にのみ、相互の機器認証が成功したものと同見做される。なお、チャレンジャーレスポンス型の機器認証については、公知であるので、説明を省略する。

【0067】両者の認証が成功した場合に、第2認証部 417 は、認証の成功を示す認証成功情報を、情報記憶部 430 へ出力する。認証が失敗した場合に、第2認証部 417 は、以降の処理を中止する。従って、ヘッドホンステレオ 500 によりメモリカード 400 から各種情報が読み出されることはない。

【0068】(13) DES 暗号化部 419

DES 暗号化部 419 は、記録データ格納部 422 からタイトル鍵及び利用条件データを読み出し、記録媒体鍵格納部 418 から記録媒体鍵を読み出す。次に、DES 暗号化部 419 は、読み出した記録媒体鍵を鍵として用いて、読み出したタイトル鍵及び利用条件データのそれぞれに、DES による暗号アルゴリズム E4 を施して、再暗号化タイトル鍵及び再暗号化利用条件データを生成し、生成した再暗号化タイトル鍵及び再暗号化利用条件データを第2記憶領域 431 へ書き込む。

【0069】1. 4 ヘッドホンステレオ 500 の構成
ヘッドホンステレオ 500 は、図 5 に示すように、第2認証部 517、記録媒体鍵取得部 518、DES 復号部 519、再暗号化データ取得部 531、記録データ格納部 532、利用条件判定部 540、DES 復号部 550 及び再生部 541 から構成されている。

【0070】(1) 記録データ格納部 532

記録データ格納部 532 は、タイトル鍵及び利用条件データを記憶するための領域を備えている。

(2) 第2認証部 517

第2認証部 517 は、メモリカード 400 が有する第2認証部 417 との間で、チャレンジャーレスポンス型の相互の機器認証を行う。具体的には、第2認証部 517 は、第2認証部 417 を認証する。次に、第2認証部 517 は、第2認証部 417 による認証を受ける。両方の認証が成功した場合にのみ、相互の機器認証が成功したものと同見做される。なお、チャレンジャーレスポンス型の機器認証については、公知であるので、説明を省略する。

【0071】両者の認証が成功した場合に、第2認証部 517 は、認証の成功を示す認証成功情報を、記録媒体

鍵取得部 518 へ出力する。認証に失敗した場合に、第2認証部 517 は、以降の処理を中止する。従って、ヘッドホンステレオ 500 が、メモリカード 400 から各種情報が読み出すことはない。

【0072】(3) 記録媒体鍵取得部 518

記録媒体鍵取得部 518 は、第2認証部 517 から認証の成功を示す認証成功情報を受け取る。認証成功情報を受け取ると、記録媒体鍵取得部 518 は、メモリカード 400 の記録媒体鍵格納部 418 から記録媒体鍵をセキュアに読み出し、読み出した記録媒体鍵を DES 復号部 519 へ出力する。

【0073】(4) 再暗号化データ取得部 531

再暗号化データ取得部 531 は、メモリカード 400 の第2記憶領域 431 から再暗号化タイトル鍵と再暗号化利用条件データとを読み出し、読み出した再暗号化タイトル鍵と再暗号化利用条件データとを DES 復号部 519 へ出力する。

(5) DES 復号部 519

DES 復号部 519 は、記録媒体鍵取得部 518 から記録媒体鍵を受け取り、再暗号化データ取得部 531 から再暗号化タイトル鍵と再暗号化利用条件データとを受け取る。次に、DES 復号部 519 は、受け取った記録媒体鍵を鍵として用いて、受け取った再暗号化タイトル鍵と再暗号化利用条件データとのそれぞれに、DES による復号アルゴリズム D4 を施して、タイトル鍵と利用条件データとを生成する。次に、生成したタイトル鍵と利用条件データとを記録データ格納部 532 へ書き込む。

【0074】ここで、復号アルゴリズム D4 は、暗号アルゴリズム E4 の逆変換を行うアルゴリズムである。

(6) 利用条件判定部 540

利用条件判定部 540 は、記録データ格納部 532 から利用条件データを読み出し、読み出した利用条件データを用いて、コンテンツの再生を許可するか否かを判断する。

【0075】具体的には、利用条件判定部 540 は、利用条件データに含まれる再生回数情報が示す回数以内の再生であれば、再生を許可する。そうでなければ、再生を許可しない。また、利用条件判定部 540 は、利用条件データに含まれる再生期間情報が示す期間内の再生であれば、再生を許可する。そうでなければ、再生を許可しない。また、利用条件判定部 540 は、利用条件データに含まれる再生累積時間情報が示す累積値以内の再生であれば、再生を許可する。そうでなければ、再生を許可しない。全ての条件において、再生を許可すると判断する場合に、再生可能を示す判断結果を生成し、いずれか一つの条件において、再生を許可しないと判断する場合に、再生不能を示す判断結果を生成する。

【0076】次に、利用条件判定部 540 は、可能であるか否かを示す判断結果を再生部 541 へ出力する。

(7) DES 復号部 550

DES復号部550は、記録データ格納部532からタイトル鍵を読み出し、メモリカード400の第1記憶領域432から暗号化コンテンツを読み出す。次に、読み出したタイトル鍵を鍵として用いて、読み出した暗号化コンテンツにDESによる復号アルゴリズムD3を施して、復号コンテンツを生成し、生成した復号コンテンツを再生部541へ出力する。

【0077】ここで、復号アルゴリズムD3は、暗号アルゴリズムE3の逆変換を行うアルゴリズムである。

(8) 再生部541

再生部541は、利用条件判定部540から判断結果を受け取り、DES復号部550から復号コンテンツを受け取る。受け取った判断結果が可能であることを示す場合に、再生部541は、受け取った復号コンテンツを再生する。

【0078】受け取った復号コンテンツが音楽である場合に、再生部541は、復号コンテンツを音楽を示すアナログの電気信号に変換し、生成したアナログの電気信号をヘッドホン700へ出力する。ヘッドホン700は、アナログの電気信号を受け取り、音声に変換して出力する。

1. 5 デジタル著作物保護システム100の動作
デジタル著作物保護システム100の動作について説明する。

【0079】(1) メモリカード400への書き込み時の動作

利用者が、PC300にメモリカード400を装着し、コンテンツ配信用サーバ装置200のコンテンツ格納部201に格納されているコンテンツ600を購入する場合の動作について、図8～図10に示すフローチャートを用いて説明する。

【0080】PC300は、利用者からコンテンツの指定を受け付け(ステップS101)、指定を受け付けたコンテンツの取得指示をインターネット10を介してコンテンツ配信用サーバ装置200へ送信する(ステップS102)。次に、コンテンツ配信用サーバ装置200がコンテンツの取得指示を受け取ると(ステップS102)、コンテンツ配信用サーバ装置200が有する第1認証部211とメモリカード400が有する第1認証部411との間で相互に機器認証を行う(ステップS103、ステップS104)。

【0081】認証に成功すると(ステップS105)、配信公開鍵取得部212は、配信公開鍵の取得指示を、インターネット10及びPC300を介して、メモリカード400の配信公開鍵格納部412へ出力する(ステップS107～ステップS108)。認証に成功すると(ステップS106)、配信公開鍵格納部412は、配信公開鍵の取得指示を受け取り(ステップS108)、次に、配信公開鍵格納部412は、配信公開鍵を読み出し(ステップS109)、読み出した配信公開鍵をPC

300及びインターネット10を介して、配信公開鍵取得部212へセキュアに出力する(ステップS110～ステップS111)。

【0082】次に、楕円暗号化部214は、配信公開鍵を鍵として用いて、タイトル鍵と利用条件鍵とを結合して暗号化し(ステップS112)、暗号化結合情報を、インターネット10及びPC300を介して、楕円復号部414へ出力する(ステップS113～ステップS114)。楕円復号部414は、暗号化結合情報を復号し(ステップS115)、タイトル鍵と利用条件鍵とを配信データ格納部423へ書き込む(ステップS116)。

【0083】次に、DES暗号化部215は、利用条件データを暗号化して(ステップS117)、暗号化利用条件データをインターネット10及びPC300を介して、DES復号部415へ出力する(ステップS118～ステップS119)。DES復号部415は、暗号化利用条件データを復号し(ステップS120)、利用条件データを配信データ格納部423へ書き込む(ステップS121)。

【0084】次に、DES暗号化部250は、コンテンツを暗号化して(ステップS122)、暗号化コンテンツをインターネット10及びPC300を介して、第1記憶領域432へ出力し(ステップS123～ステップS124)、第1記憶領域432は、暗号化コンテンツを記憶する(ステップS125)。次に、変換部416は、配信データ格納部423に記憶されている配信用データを変換して、記録データを生成し、生成した記録データを記録データ格納部422へ書き込む(ステップS126)。次に、DES暗号化部419は、記録データ格納部422に記録されているタイトル鍵と利用条件データとをそれぞれ暗号化し(ステップS127)、再暗号化タイトル鍵と再暗号化利用条件データとを第2記憶領域431へ書き込む(ステップS128)。

【0085】(2) メモリカード400からの読み出し時の動作

次に、利用者が、PC300からメモリカード400を抜き出し、抜き出したメモリカード400をヘッドホンステレオ500に装着して、コンテンツを再生する場合における動作について、図11～図12に示すフローチャートを用いて説明する。

【0086】ヘッドホンステレオ500が利用者からコンテンツの再生指示を受け付けると(ステップS201)、ヘッドホンステレオが有する第2認証部517とメモリカード400が有する第2認証部417との間で相互に機器認証を行う(ステップS202、ステップS203)。認証に成功すると(ステップS205)、記録媒体鍵取得部518は、記録媒体鍵を取得する旨の指示を記録媒体鍵格納部418へ出力する(ステップS206)。

【0087】認証に成功すると（ステップS204）、記録媒体鍵格納部418は、記録媒体鍵を取得する旨の指示を受け取り（ステップS206）、記録媒体鍵格納部418は、記録媒体鍵を読み出し（ステップS207）、読み出した記録媒体鍵を記録媒体鍵取得部518へ出力する（ステップS208）。次に、再暗号化データ取得部531は、再暗号化データを取得する旨の指示を第2記憶領域431へ出力し（ステップS209）、第2記憶領域431は、再暗号化タイトル鍵と再暗号化利用条件データとを読み出し（ステップS210）、読み出した再暗号化タイトル鍵と再暗号化利用条件データとを再暗号化データ取得部531へ出力する（ステップS211）。次に、DES復号部519は、再暗号化タイトル鍵と再暗号化利用条件データとを復号し、記録データ格納部532へ書き込む（ステップS212）。

【0088】第1記憶領域432は、暗号化コンテンツを読み出し（ステップS213）、読み出した暗号化コンテンツをDES復号部550へ出力し（ステップS214）、DES復号部550は、暗号化コンテンツを復号する（ステップS215）。利用条件判定部540は、記録データ格納部532から利用条件データを読み出し、読み出した利用条件データによりコンテンツの再生が許可されているか否かを判定し、許可されている場合に（ステップS216）、再生部541は、復号して生成されたコンテンツを再生する（ステップS217）。

【0089】1.6 まとめ

以上説明したように、暗号化タイトル鍵及び利用条件データの復号及び再暗号化（暗号変換）を記録媒体装置の耐タンパモジュール部で行うことにより、不正な第三者によるハッキングを困難にすることが可能となる。

2. 実施の形態2

本発明に係る別の実施の形態としてのデジタル著作物保護システム100b（図示していない）について説明する。

【0090】デジタル著作物保護システム100bは、デジタル著作物保護システム100と同様の構成を有しており、コンテンツ配信用サーバ装置200に代えてコンテンツ配信用サーバ装置200bを備え、メモリカード400に代えてメモリカード400bを備えている。ここでは、デジタル著作物保護システム100との相違点を中心として説明する。

【0091】2.1 コンテンツ配信用サーバ装置200b

コンテンツ配信用サーバ装置200bは、コンテンツ配信用サーバ装置200と同様の構成を有しており、図13に示すように、第1認証部211、配信公開鍵取得部212、配信データ格納部202、楕円暗号化部214、ハッシュ部220、コンテンツ格納部201、DES暗号化部250及び書込部221から構成されてい

る。ここでは、コンテンツ配信用サーバ装置200との相違点を中心として説明する。

【0092】（1）配信データ格納部202

配信データ格納部202は、図16に示すように、タイトル鍵、ダイジェスト及び利用条件データを記憶するための領域を備えており、あらかじめタイトル鍵及び利用条件データを記憶している。タイトル鍵、ダイジェスト及び利用条件データは、コンテンツ格納部201が記憶しているコンテンツ600に対応している。

10 【0093】タイトル鍵及び利用条件データについては、上述しているので、説明を省略する。ダイジェストは、利用条件データに対してハッシュ関数を施して得られた値であり、ハッシュ部220により配信データ格納部202に書き込まれる。

（2）第1認証部211

第1認証部211は、認証の成功を示す認証成功情報を、配信公開鍵取得部212及び楕円暗号化部214へ出力する。

【0094】（3）ハッシュ部220

20 ハッシュ部220は、配信データ格納部202から利用条件データを読み出し、読み出した利用条件データにハッシュ関数F1を施して、ダイジェストを生成し、生成したダイジェストを配信データ格納部202へ書き込む。ここで、ハッシュ関数F1としては具体的には米国標準のSHAアルゴリズムなどを利用することができる。SHAアルゴリズムについては、例えば岡本栄司著「暗号理論入門」（共立出版株式会社）に詳細に説明されている。

【0095】（4）楕円暗号化部214

30 楕円暗号化部214は、配信データ格納部202からタイトル鍵とダイジェストとを読み出す。次に、楕円暗号化部214は、受け取った前記配信公開鍵を鍵として用いて、タイトル鍵とダイジェストとを結合した結合情報に、楕円暗号方式による暗号アルゴリズムE1を施して暗号化結合情報を生成する。

【0096】（5）書込部221

40 書込部221は、配信データ格納部202から利用条件データを読み出し、読み出した利用条件データを、インターネット10及びPC300を介して、メモリカード400bの配信データ格納部423内に書き込む。

2.2 メモリカード400b

50 メモリカード400bは、メモリカード400と同様の構成を有しており、図14に示すように、外部から読み書きできない耐タンパモジュール部410bと情報記憶部430とから構成されており、耐タンパモジュール部410bは、第1認証部411、配信公開鍵格納部412、配信秘密鍵格納部413、楕円復号部414、変換部416、第2認証部417、記録媒体鍵格納部418、DES暗号化部419、ハッシュ部420、比較部421、配信データ格納部423及び記録データ格納部

422から構成されている。ここでは、メモリカード400との相違点を中心として説明する。

【0097】(1) 楕円復号部414

楕円復号部414は、読み出した配信秘密鍵を鍵として用いて、受け取った暗号化結合情報に楕円暗号方式による復号アルゴリズムD1を施して、タイトル鍵及びダイジェストを生成し、生成したタイトル鍵及びダイジェストを配信データ格納部423へ書き込む。

【0098】(2) ハッシュ部420

ハッシュ部420は、配信データ格納部423からよ利用条件データを読み出し、読み出した利用条件データにハッシュ関数F1を施して、ダイジェストを生成し、生成したダイジェストを比較部421へ出力する。ここで、ハッシュ関数F1は、コンテンツ配信用サーバ装置200bが有するハッシュ部220において用いられたハッシュ関数F1と同一のものである。

【0099】(3) 比較部421

比較部421は、配信データ格納部423からダイジェストを読み出し、ハッシュ部420からダイジェストを受け取る。次に、比較部421は、読み出したダイジェストと受け取ったダイジェストとが一致しているか否かを判断し、一致又は不一致を示す判断情報を変換部416へ出力する。

【0100】(4) 変換部416

変換部416は、比較部421から判断情報を受け取る。判断情報が一致を示す場合には、変換部416は、配信データ格納部423からタイトル鍵及び利用条件データを読み出し、読み出したタイトル鍵及び利用条件データをこの順序で、記録データ格納部422へ書き込む。記録データ格納部422に書き込まれるタイトル鍵及び利用条件データを図17に示す。

【0101】判断情報が不一致を示す場合には、変換部416は、なにもしない。従って、この場合には、タイトル鍵と利用条件データとは、記録データ格納部422へ書き込まれない。

2. 3 ヘッドホンステレオ500の構成

ヘッドホンステレオ500は、図15に示すように、第2認証部517、記録媒体鍵取得部518、DES復号部519、再暗号化データ取得部531、記録データ格納部532、利用条件判定部540、DES復号部550及び再生部541から構成されており、デジタル著作権保護システム100のヘッドホンステレオ500と同じ構成を有するので、説明を省略する。

【0102】2. 4 デジタル著作権保護システム100bの動作

デジタル著作権保護システム100bの動作について説明する。

(1) メモリカード400bへの書き込み時の動作

利用者が、PC300にメモリカード400bを装着し、コンテンツ配信用サーバ装置200bのコンテンツ

格納部201に格納されているコンテンツ600を購入する場合の動作について、図18～図20に示すフローチャートを用いて説明する。

【0103】PC300は、利用者からコンテンツの指定を受け付け（ステップS301）、指定を受け付けたコンテンツの取得指示をインターネット10を介してコンテンツ配信用サーバ装置200bへ送信する（ステップS302）。次に、コンテンツ配信用サーバ装置200bがコンテンツの取得指示を受け取ると（ステップS302）、コンテンツ配信用サーバ装置200bが有する第1認証部211とメモリカード400bが有する第1認証部411との間で相互に機器認証を行う（ステップS303、ステップS304）。

【0104】認証に成功すると（ステップS305）、配信公開鍵取得部212は、配信公開鍵の取得指示を、インターネット10及びPC300を介して、メモリカード400bの配信公開鍵格納部412へ出力する（ステップS307～ステップS308）。認証に成功すると（ステップS306）、配信公開鍵格納部412は、配信公開鍵の取得指示を受け取り（ステップS308）、次に、配信公開鍵格納部412は、配信公開鍵を読み出し（ステップS309）、読み出した配信公開鍵をPC300及びインターネット10を介して、配信公開鍵取得部212へ出力する（ステップS310～ステップS311）。

【0105】次に、ハッシュ部220は、利用条件データを読み出し、読み出した利用条件データにハッシュ関数F1を施してダイジェストを生成し（ステップS312）、生成したダイジェストを配信データ格納部202へ書き込む（ステップS313）。次に、楕円暗号化部214は、配信公開鍵を鍵として用いて、タイトル鍵とダイジェストとを結合して暗号化し（ステップS314）、暗号化結合情報を、インターネット10及びPC300を介して、楕円復号部414へ出力する（ステップS315～ステップS316）。

【0106】楕円復号部414は、暗号化結合情報を復号し（ステップS317）、タイトル鍵とダイジェストとを配信データ格納部423へ書き込む（ステップS318）。書込部221は、利用条件データを読み出して、読み出した利用条件データをインターネット10及びPC300を介して、配信データ格納部423へ書き込む（ステップS319～ステップS320）。

【0107】次に、DES暗号化部250は、コンテンツを暗号化して（ステップS322）、暗号化コンテンツをインターネット10及びPC300を介して、第1記憶領域432へ出力し（ステップS323～ステップS324）、第1記憶領域432は、暗号化コンテンツを記憶する（ステップS325）。次に、ハッシュ部420は、配信データ格納部423から利用条件データを読み出し、読み出した利用条件データにハッシュ関数F

1を施してダイジェストを生成し、生成したダイジェストを比較部421へ出力する(ステップS326)。次に、比較部421は、配信データ格納部423からダイジェストを読み出し、ハッシュ部420からダイジェストを受け取り、読み出したダイジェストと受け取ったダイジェストとが一致しているか否かを判断し、一致又は不一致を示す判断情報を変換部416へ出力し、変換部416は、比較部421から判断情報を受け取り、判断情報が一致を示す場合には(ステップS327)、変換部416は、配信データ格納部423からタイトル鍵及び利用条件データを読み出し、読み出したタイトル鍵及び利用条件データをこの順序で、記録データ格納部422へ書き込む(ステップS328)。次に、DES暗号化部419は、記録データ格納部422に記録されているタイトル鍵と利用条件データとをそれぞれ暗号化し(ステップS329)、再暗号化タイトル鍵と再暗号化利用条件データとを第2記憶領域431へ書き込む(ステップS330)。

【0108】変換部416は、比較部421から受け取った判断情報が不一致を示す場合には(ステップS327)、なにもしないで、処理を終了する。

(2) メモリカード400bからの読み出し時の動作
次に、利用者が、PC300からメモリカード400bを抜き出し、抜き出したメモリカード400bをヘッドホンステレオ500に装着して、コンテンツを再生する場合における動作については、図11～図12のフローチャートに示す動作と同じであるので、説明を省略する。

【0109】2. 5 まとめ

以上説明したように、暗号化タイトル鍵及び利用条件データの復号及び再暗号化(暗号変換)を記録媒体装置が有する耐タンパモジュール部で行うことにより、不正な第三者によるハッキングを困難にすることが可能となる。

3. 実施の形態3

本発明の別の実施の形態としてのデジタル著作物保護システム100c(図示していない)について説明する。

【0110】デジタル著作物保護システム100cは、デジタル著作物保護システム100と同様の構成を有しており、コンテンツ配信用サーバ装置200に代えてコンテンツ配信用サーバ装置200cを備え、メモリカード400に代えてメモリカード400cを備えている。ここでは、デジタル著作物保護システム100との相違点を中心として説明する。

【0111】3. 1 コンテンツ配信用サーバ装置200c

コンテンツ配信用サーバ装置200cは、コンテンツ配信用サーバ装置200が備える構成要素に加えて、さらに、図21に示すように、鍵記憶部261、情報記憶部262、ハッシュ部263、暗号化部264及び送受信

部265を含んでいる。

【0112】(1) 情報記憶部262

情報記憶部262は、あらかじめ更新モジュールを記憶している。更新モジュールは、メモリカードが有する耐タンパモジュール部内に含まれているコンピュータプログラムやデータなどを更新するための情報である。具体的には、前記更新モジュールは、耐タンパモジュール部内に含まれる暗号化方式、復号方式及び変換方式を更新するためのものである。

10 【0113】(2) 鍵記憶部261

鍵記憶部261は、あらかじめ判定鍵を記憶している。判定鍵は、64ビット長の情報である。

(3) ハッシュ部263

ハッシュ部263は、情報記憶部262から更新モジュールを読み出し、読み出した更新モジュールにハッシュ関数F2を施して第1ハッシュ値を生成し、生成した第1ハッシュ値を暗号化部264へ出力する。

【0114】(4) 暗号化部264

20 暗号化部264は、鍵記憶部261から判定鍵を読み出し、ハッシュ部263から第1ハッシュ値を受け取る。次に、暗号化部264は、読み出した判定鍵を鍵として用いて、受け取った第1ハッシュ値に暗号アルゴリズムE5を施して暗号化ハッシュ値を生成し、生成した暗号化ハッシュ値を、インターネット10及びPC300を介して、メモリカード400cの復号部462(後述する)へ送信する。

【0115】(5) 送受信部265

送受信部265は、情報記憶部262から更新モジュールを読み出し、読み出した更新モジュールを、インターネット10及びPC300を介して、メモリカード400cの送受信部463(後述する)へ送信する。

3. 2 メモリカード400c

メモリカード400cは、耐タンパモジュール部410に代えて、耐タンパモジュール部410cを備えている。

【0116】耐タンパモジュール部410cは、耐タンパモジュール部410が備える構成要素に加えて、さらに、図21に示すように、鍵記憶部461、復号部462、送受信部463、ハッシュ部464、判定部465及び更新部466を備えている。

(1) 鍵記憶部461

40 鍵記憶部461は、あらかじめ判定鍵を記憶している。判定鍵は、64ビット長の情報である。この判定鍵は、鍵記憶部261が記憶している判定鍵と同じものである。

【0117】(2) 復号部462

50 復号部462は、コンテンツ配信用サーバ装置200cから、インターネット10及びPC300を介して、暗号化ハッシュ値を受け取り、鍵記憶部461から判定鍵を読み出す。次に、復号部462は、読み出した判定鍵

を鍵として用いて、受け取った暗号化ハッシュ値に復号アルゴリズムD5を施して第1ハッシュ値を生成し、生成した第1ハッシュ値を判定部465へ出力する。

【0118】ここで、復号アルゴリズムD5は、暗号アルゴリズムE5の逆変換を行うアルゴリズムである。

(3) 送受信部463

送受信部463は、コンテンツ配信用サーバ装置200cから、インターネット10及びPC300を介して、更新モジュールを受け取り、受け取った更新モジュールをハッシュ部464及び更新部466へ出力する。

【0119】(4) ハッシュ部464

ハッシュ部464は、送受信部463から更新モジュールを受け取り、受け取った更新モジュールにハッシュ関数F2を施して第2ハッシュ値を生成し、生成した第2ハッシュ値を判定部465へ出力する。

(5) 判定部465

判定部465は、復号部462から第1ハッシュ値を受け取り、ハッシュ部464から第2ハッシュ値を受け取る。次に、判定部465は、受け取った第1ハッシュ値と受け取った第2ハッシュ値とが一致するか否かを判定し、一致するか否かを示す判定情報を更新部466へ出力する。

【0120】(6) 更新部466

更新部466は、送受信部463から更新モジュールを受け取り、判定部465から判定情報を受け取る。受け取った判定情報が一致することを示す場合に、更新部466は、受け取った更新モジュールを用いて、耐タンパモジュール部410c内に記憶されているコンピュータプログラム又はデータを更新する。

【0121】3. 3 デジタル著作物保護システム100cの動作

デジタル著作物保護システム100cにおいて、メモリカード400c内の耐タンパモジュール部410cに含まれるコンピュータ又はデータを更新する場合の動作について、図22に示すフローチャートを用いて説明する。コンテンツ配信用サーバ装置200cにおいて、ハッシュ部263は、情報記憶部262から更新モジュールを読み出し、読み出した更新モジュールにハッシュ関数F2を施して第1ハッシュ値を生成し、生成した第1ハッシュ値を暗号化部264へ出力する(ステップS401)。次に、暗号化部264は、鍵記憶部261から判定鍵を読み出し、ハッシュ部263から第1ハッシュ値を受け取り、読み出した判定鍵を鍵として用いて、受け取った第1ハッシュ値に暗号アルゴリズムE5を施して暗号化ハッシュ値を生成する(ステップS402)。次に、暗号化部264は、生成した暗号化ハッシュ値を、インターネット10及びPC300を介して、メモリカード400cの復号部462へ送信し、送受信部265は、情報記憶部262から更新モジュールを読み出し、読み出した更新モジュールを、インターネット10

及びPC300を介して、メモリカード400cの送受信部463へ送信する(ステップS403、ステップS404)。

【0122】次に、メモリカード400cにおいて、復号部462は、コンテンツ配信用サーバ装置200cから、インターネット10及びPC300を介して、暗号化ハッシュ値を受け取り、送受信部463は、コンテンツ配信用サーバ装置200cから、インターネット10及びPC300を介して、更新モジュールを受け取る(ステップS403、ステップS404)。次に、復号部462は、鍵記憶部461から判定鍵を読み出し、読み出した判定鍵を鍵として用いて、受け取った暗号化ハッシュ値に復号アルゴリズムD5を施して第1ハッシュ値を生成し、生成した第1ハッシュ値を判定部465へ出力する(ステップS405)。次に、ハッシュ部464は、送受信部463から更新モジュールを受け取り、受け取った更新モジュールにハッシュ関数F2を施して第2ハッシュ値を生成し、生成した第2ハッシュ値を判定部465へ出力する(ステップS406)。次に、判定部465は、受け取った第1ハッシュ値と受け取った第2ハッシュ値とが一致するか否かを判定し、一致するか否かを示す判定情報を更新部466へ出力し、受け取った判定情報が一致することを示す場合に(ステップS407)、更新部466は、受け取った更新モジュールを用いて、耐タンパモジュール部410c内に記憶されているコンピュータプログラム又はデータを更新する(ステップS408)。

【0123】受け取った判定情報が一致しないことを示す場合に(ステップS407)、更新部466は、なにもしないで、処理を終了する。

3. 6 まとめ

従来のシステムでは、予め定められた配信データフォーマット及び配信用暗号方式に従って、タイトル鍵や利用条件データが暗号化され、ユーザのパソコン上で、暗号化されたタイトル鍵や利用条件データが復号された後、予め定められた記録データフォーマットや記録用暗号方式に従って再暗号化されて記録媒体に記録されることが行われている。

【0124】しかしこのパソコン上で行われている暗号変換やデータフォーマットの変換を記録媒体装置が有する耐タンパモジュールで実現した場合、将来異なる配信用暗号方式や異なる配信データフォーマットに従ったコンテンツに容易に対応することができない。この対策として、本発明は、記録媒体装置上での暗号変換やフォーマット変換を行う耐タンパモジュールを安全に更新可能なデジタル著作物保護システム、記録媒体装置、サーバ装置、及び再生装置を提供することを目的とする。

【0125】4. 総括

以上説明したように、本発明は、デジタル著作物であるコンテンツを扱うデジタル著作物保護システムであっ

て、サーバ装置と、記録媒体装置と、再生装置とからなる。前記サーバ装置は、前記コンテンツをコンテンツ毎に固有に暗号化して暗号化コンテンツを生成する第1の暗号化手段と、予め定められた配信データフォーマットに従って、コンテンツの利用条件を表す利用条件データを記録媒体装置毎に固有に暗号化して暗号化利用条件データを生成する第2の暗号化手段とを備える。前記記録媒体装置は、前記サーバ装置から前記暗号化コンテンツと、前記暗号化利用条件データを取得する取得手段と、前記取得手段で取得した暗号化コンテンツを格納する第1の記憶領域と、前記取得手段で取得した暗号化利用条件データを復号する、前記第2の暗号化手段に対応する第2の復号手段と、前記第2の復号手段で復号された前記利用条件データを、前記配信データフォーマットから予め定められた記録データフォーマットに変換するデータフォーマット変換手段と、前記データフォーマット変換手段で変換された利用条件データを記録媒体装置毎に固有に暗号化して再暗号化利用条件データを生成する第3の暗号化手段と、前記再暗号化利用条件データを格納する第2の記憶領域とを備え、前記第2の復号手段と前記データフォーマット変換手段と前記第3の暗号化手段が、耐タンパ性のある耐タンパモジュールにより構成されている。前記再生装置は、前記記録媒体装置の第1の記憶領域に格納された暗号化コンテンツと、前記記録媒体装置の第2の記憶領域に格納された再暗号化利用条件データを読み出す読み出し手段と、前記読み出し手段で読み出した前記再暗号化利用条件データを復号する、前記第3の暗号化手段に対応する第3の復号手段と、前記読み出し手段で読み出した暗号化コンテンツを復号する、前記第1の暗号化手段に対応する第1の復号手段と、前記第1の復号手段で復号されたコンテンツを前記第3の復号手段で復号された利用条件データによって許諾された範囲で再生するための再生手段とを備えている。

【0126】ここで、前記サーバ装置は、さらに、前記記録媒体装置の配信用秘密鍵記憶領域に格納された、前記記録媒体装置に固有の配信用秘密鍵に対応する配信用公開鍵をセキュアに取得する配信用公開鍵取得手段を備え、前記第1の暗号化手段は、コンテンツを、コンテンツ毎に固有のタイトル鍵を用いて共通鍵暗号方式によって暗号化して暗号化コンテンツを生成し、前記第2の暗号化手段は、前記タイトル鍵及び利用条件データを、配信用公開鍵取得手段で取得した前記配信用公開鍵を用いて公開鍵暗号方式によって暗号化して暗号化タイトル鍵及び暗号化利用条件データを生成する。前記記録媒体装置は、さらに、前記配信用公開鍵に対応する配信用秘密鍵を格納する配信用秘密鍵記憶領域と、記録媒体装置毎に固有の記録用媒体固有鍵を格納する記録用媒体固有鍵記憶領域とを備え、前記取得手段は、前記サーバ装置から暗号化コンテンツと、暗号化タイトル鍵及び暗号化利

用条件データを取得し、前記第2の復号手段は、前記配信用秘密鍵記憶領域に格納された配信用秘密鍵を用いて前記公開鍵暗号方式を利用して前記暗号化タイトル鍵及び暗号化利用条件データを復号し、前記第3の暗号化手段は、復号された前記タイトル鍵及び前記利用条件データを前記記録用媒体固有鍵記憶領域に格納された記録用媒体固有鍵を用いて共通鍵暗号方式によって暗号化して再暗号化タイトル鍵及び再暗号化利用条件データを生成するものとし、前記第2の復号手段と前記データフォーマット変換手段と前記第3の暗号化手段に加えて、前記配信用秘密鍵記憶領域、及び、前記記録用媒体固有鍵記憶領域が、耐タンパ性のある耐タンパモジュールにより構成されている。前記再生装置は、さらに、前記記録媒体装置の記録用媒体固有鍵記憶領域に格納された記録用媒体固有鍵をセキュアに取得する媒体固有鍵取得手段を備え、前記読み出し手段は、前記再暗号化タイトル鍵及び再暗号化利用条件データを前記記録媒体装置から読み出し、前記第3の復号手段は、前記読み出し手段で読み出した前記再暗号化タイトル鍵及び再暗号化利用条件データを前記媒体固有鍵で前記共通鍵暗号方式によって復号し、前記第1の復号手段は、前記暗号化コンテンツを、前記タイトル鍵を用いて前記共通鍵暗号方式によって復号し、前記再生手段は、前記利用条件データによって許諾された範囲で復号されたコンテンツを再生する。

【0127】ここで、前記サーバ装置の前記前記第2の暗号化手段は、前記タイトル鍵と、利用条件データのダイジェスト値もしくは利用条件データの暗号化及び復号に用いる利用条件用鍵の少なくとも一方を含む利用条件関連情報を、前記配信用公開鍵を用いて公開鍵暗号方式によって暗号化して暗号化タイトル鍵及び暗号化利用条件関連情報を生成し、前記利用条件関連情報が前記利用条件データのダイジェスト値を含む場合は、前記利用条件データをハッシュ関数を利用して前記利用条件データのダイジェスト値を生成し、もしくは、前記利用条件関連情報が前記利用条件用鍵を含む場合は、前記利用条件データを前記利用条件用鍵を用いて共通鍵暗号方式で暗号化し、前記記録媒体装置の前記取得手段は、前記サーバ装置から、暗号化タイトル鍵及び暗号化利用条件関連情報を取得し、さらに、前記利用条件関連情報に利用条件データのダイジェスト値のみが含まれる場合は、前記利用条件データを取得し、前記利用条件関連情報に利用条件用鍵が含まれる場合は、前記暗号化利用条件データを取得し、前記第2の復号手段は、前記暗号化タイトル鍵及び暗号化利用条件関連情報を、前記配信用秘密鍵を用いて公開鍵暗号方式によって復号し、復号された前期利用条件関連情報に利用条件用鍵が含まれる場合は、前記暗号化利用条件データを前記利用条件用鍵を用いて共通鍵方式で復号して利用条件データを得ること、もしくは、前期利用条件関連情報に利用条件データのダイジェスト値が含まれる場合は、前記利用条件データを前記ハ

ッシュ関数を利用して前記利用条件データの参照用ダイジェスト値を生成し、この参照用ダイジェスト値が、前記利用条件関連情報に含まれる利用条件データのダイジェスト値と一致するかどうか判定する。

【0128】ここで、前記記録媒体装置と前記サーバ装置は、それぞれ、さらに第1の認証手段を備え、前記サーバ装置は、前記記録媒体装置から前記配信用公開鍵を取得するのに先立って、もしくは、前記記録媒体装置は、前記サーバ装置から暗号化タイトル鍵及び暗号化利用条件データを取得するのに先立って、前記サーバ装置の第1の認証手段は、前記記録媒体装置の正当性を認証し、前記記録媒体装置の第1の認証手段は、前記サーバ装置の正当性を認証し、それぞれの認証が成功した場合に、前記サーバ装置は、前記記録媒体装置から前記配信用公開鍵を取得する、もしくは、前記記録媒体装置は、前記暗号化タイトル鍵及び暗号化利用条件データを取得する。

【0129】ここで、前記記録媒体装置と前記再生装置は、それぞれ、さらに第2の認証手段を備え、前記再生装置は、前記記録媒体装置から、前記媒体固有鍵を取得するのに先立って、もしくは、前記記録媒体装置は、前記再生装置から、前記暗号化タイトル鍵及び暗号化利用条件データが読み出されるのに先立って、前記再生装置の第2の認証手段は、前記記録媒体装置を認証し、前記記録媒体装置の第2の認証手段は、前記再生装置の正当性を認証し、それぞれの認証が成功した場合に、前記再生装置は、前記記録媒体装置から、前記媒体固有鍵を取得する、もしくは、前記記録媒体装置から、前記暗号化利用条件データが読み出される。

【0130】ここで、前記サーバ装置は、前記記録媒体装置の配信用秘密鍵が暴露された場合に、前記配信用秘密鍵に対応する配信用公開鍵をリボークリストに登録し、前記リボークリストに登録された配信用公開鍵を用いて前記タイトル鍵及び前記利用条件データを暗号化して前記記録媒体装置に提供することを禁止する。ここで、前記利用条件データは、前記コンテンツの再生回数を制御する情報、もしくは、前記コンテンツの再生期間を制御する情報、もしくは、前記コンテンツの再生累積時間を制御する情報を含む。

【0131】ここで、前記耐タンパモジュールが、耐タンパ性のあるハードウェア、もしくは、耐タンパ性のあるソフトウェア、もしくは、両者の組み合わせで構成される。また、本発明は、デジタル著作物であるコンテンツを記録するための記録媒体装置であって、暗号化コンテンツと、暗号化利用条件データを取得する取得手段と、前記取得手段で取得した暗号化コンテンツを格納する第1の記憶領域と、前記取得手段で取得した暗号化利用条件データを復号する第2の復号手段と、前記第2の復号手段で復号された利用条件データを、予め定められた配信データフォーマットから予め定められた記録デー

タフォーマットに変換するデータフォーマット変換手段と、前記データフォーマット変換手段で変換された利用条件データを記録媒体装置毎に固有に暗号化して再暗号化利用条件データを生成する第3の暗号化手段と、第3の暗号化手段で暗号化された再暗号化利用条件データを格納する第2の記憶領域とを備え、前記第2の復号手段と前記データフォーマット変換手段と前記第3の暗号化手段が、耐タンパ性のある耐タンパモジュールにより構成される。

【0132】ここで、前記記録媒体装置は、さらに、前記配信用公開鍵に対応する配信用秘密鍵を格納する配信用秘密鍵記憶領域と、記録媒体装置毎に固有の記録用媒体固有鍵を格納する記録用媒体固有鍵記憶領域とを備え、前記取得手段は、前記サーバ装置から暗号化コンテンツと、暗号化タイトル鍵及び暗号化利用条件データを取得し、前記第2の復号手段は、前記配信用秘密鍵記憶領域に格納された配信用秘密鍵を用いて前記公開鍵暗号方式を利用して前記暗号化タイトル鍵及び暗号化利用条件データを復号し、前記第3の暗号化手段は、復号された前記タイトル鍵及び前記利用条件データを前記記録用媒体固有鍵記憶領域に格納された記録用媒体固有鍵を用いて共通鍵暗号方式によって暗号化して再暗号化タイトル鍵及び再暗号化利用条件データを生成するものとし、前記第2の復号手段と前記データフォーマット変換手段と前記第3の暗号化手段に加えて、前記配信用秘密鍵記憶領域、及び、前記記録用媒体固有鍵記憶領域が、耐タンパ性のある耐タンパモジュールにより構成される。

【0133】ここで、前記記録媒体装置の前記取得手段は、前記サーバ装置から、暗号化タイトル鍵及び暗号化利用条件関連情報を取得し、さらに、前記利用条件関連情報に利用条件データのダイジェスト値のみが含まれる場合は、前記利用条件データを取得し、前記利用条件関連情報に利用条件用鍵が含まれる場合は、前記暗号化利用条件データを取得し、前記第2の復号手段は、前記暗号化タイトル鍵及び暗号化利用条件関連情報を、前記配信用秘密鍵を用いて公開鍵暗号方式によって復号し、復号された前期利用条件関連情報に利用条件用鍵が含まれる場合は、前記暗号化利用条件データを前記利用条件用鍵を用いて共通鍵方式で復号して利用条件データを得ること、もしくは、前期利用条件関連情報に利用条件データのダイジェスト値が含まれる場合は、前記利用条件データを前記ハッシュ関数を利用して前記利用条件データの参照用ダイジェスト値を生成し、この参照用ダイジェスト値が、前記利用条件関連情報に含まれる利用条件データのダイジェスト値と一致するかどうか判定する。

【0134】ここで、前記記録媒体装置は、さらに第1の認証手段と第2の認証手段を備え、前記記録媒体装置は、前記サーバ装置によって、前記配信用公開鍵が取得されるのに先立って、もしくは、前記記録媒体装置は、前記サーバ装置から暗号化タイトル鍵及び暗号化利用条

件データを取得するのに先立って、前記サーバ装置の第 1 の認証手段は、前記記録媒体装置の正当性を認証し、前記記録媒体装置の第 1 の認証手段は、前記サーバ装置の正当性を認証し、それぞれの認証が成功した場合に、前記記録媒体装置は、前記サーバ装置によって前記配信用公開鍵が取得され、もしくは、前記記録媒体装置は、前記暗号化タイトル鍵及び暗号化利用条件データを取得し、前記記録媒体装置は、前記再生装置によって前記媒体固有鍵が取得されるのに先立って、もしくは、前記記録媒体装置は、前記再生装置から、前記暗号化タイトル鍵及び暗号化利用条件データが読み出されるのに先立って、前記再生装置の第 2 の認証手段は、前記記録媒体装置を認証し、前記記録媒体装置の第 2 の認証手段は、前記再生装置の正当性を認証し、それぞれの認証が成功した場合に、前記記録媒体装置は、前記再生装置によって前記媒体固有鍵が取得される、もしくは、前記記録媒体装置から、前記暗号化利用条件が読み出される。

【0135】ここで、前記配信データフォーマット、もしくは、前記記録データフォーマットの変更があった時に、前記記録媒体装置の前記データフォーマット変換手段を構成する耐タンパモジュールを更新する。ここで、前記記録媒体装置の第 2 の復号手段が利用する暗号方式、もしくは、前記第 3 の暗号化手段が利用する暗号方式の変更があった時に、前記第 2 の復号手段、もしくは、前記第 3 の暗号化手段を構成する耐タンパモジュールを更新する。

【0136】ここで、前記記録媒体装置は、さらに、更新する耐タンパモジュールの正当性を判定する耐タンパモジュール判定手段を備え、前記耐タンパモジュール判定手段が、耐タンパモジュールの正当と判定した場合に耐タンパモジュールを更新する。ここで、前記記録媒体装置の前記第 2 の復号手段は、複数の暗号方式から一つを選択して復号することを可能とし、前記第 3 の暗号化手段は、複数の暗号方式から一つを選択して復号する。

【0137】ここで、前記記録媒体装置の前記配信用鍵記憶領域は、複数の配信用秘密鍵を格納し、前記第 2 の復号手段は、複数の配信用秘密鍵から一つを選択利用する。ここで、前記耐タンパモジュールが、耐タンパ性のあるハードウェア、もしくは、耐タンパ性のあるソフトウェア、もしくは、両者の組み合わせで構成される。

【0138】また、本発明は、デジタル著作物であるコンテンツを記録媒体装置に提供するためのサーバ装置であって、コンテンツをコンテンツ毎に固有に暗号化して暗号化コンテンツを生成する第 1 の暗号化手段と、予め定められた配信フォーマットに従って、コンテンツの利用条件を表す利用条件データを記録媒体装置毎に固有に暗号化して暗号化利用条件データを生成する第 2 の暗号化手段とを備える。

【0139】ここで、前記サーバ装置は、さらに、前記記録媒体装置の配信用秘密鍵記憶領域に格納された、前

記記録媒体装置に固有の配信用秘密鍵に対応する配信用公開鍵をセキュアに取得する配信用公開鍵取得手段を備え、前記第 1 の暗号化手段は、コンテンツを、コンテンツ毎に固有のタイトル鍵を用いて共通鍵暗号方式によって暗号化して暗号化コンテンツを生成し、前記第 2 の暗号化手段は、前記タイトル鍵及び利用条件データを、配信用公開鍵取得手段で取得した前記配信用公開鍵を用いて公開鍵暗号方式によって暗号化して暗号化タイトル鍵及び暗号化利用条件データを生成する。

10 【0140】ここで、前記サーバ装置の前記前記第 2 の暗号化手段は、前記タイトル鍵と、利用条件データのダイジェスト値もしくは利用条件データの暗号化及び復号に用いる利用条件用鍵の少なくとも一方を含む利用条件関連情報を、前記配信用公開鍵を用いて公開鍵暗号方式によって暗号化して暗号化タイトル鍵及び暗号化利用条件関連情報を生成し、前記利用条件関連情報が前記利用条件データのダイジェスト値を含む場合は、前記利用条件データをハッシュ関数を利用して前記利用条件データのダイジェスト値を生成し、もしくは、前記利用条件関連情報が前記利用条件用鍵を含む場合は、前記利用条件データを前記利用条件用鍵を用いて共通鍵暗号方式で暗号化する。

20 【0141】ここで、前記サーバ装置は、さらに第 1 の認証手段を備え、前記サーバ装置は、前記記録媒体装置から前記配信用公開鍵を取得するのに先立って、もしくは、前記サーバ装置は、前記記録媒体装置によって暗号化タイトル鍵及び暗号化利用条件データが取得されるのに先立って、前記サーバ装置の第 1 の認証手段は、前記記録媒体装置の正当性を認証し、前記記録媒体装置の第 1 の認証手段は、前記サーバ装置の正当性を認証し、それぞれの認証が成功した場合に、前記サーバ装置は、前記記録媒体装置から前記配信用公開鍵を取得する、もしくは、前記サーバ装置は、前記記録媒体装置によって暗号化タイトル鍵及び暗号化利用条件データが取得される。

30 【0142】ここで、前記サーバ装置の前記第 2 の暗号化手段は、前記記録媒体装置の配信用秘密鍵が暴露された場合に、前記配信用秘密鍵に対応する配信用公開鍵をリボークリストに登録し、前記リボークリストに登録した配信用公開鍵を用いて前記タイトル鍵及び前記利用条件データを暗号化して前記記録媒体装置に提供することを禁止する。

40 【0143】また、本発明は、デジタル著作物であるコンテンツを記録媒体装置から読み出して再生するための再生装置であって、前記再生装置は、前記記録媒体装置の第 1 の記憶領域に格納された暗号化コンテンツと、記録媒体装置の第 2 の記憶領域に格納された再暗号化利用条件データを読み出す読み出し手段と、前記読み出し手段で読み出した前記再暗号化利用条件データを復号する、記録媒体装置の第 3 の暗号化手段に対応する第 3 の

復号手段と、前記読み出し手段で読み出した前記暗号化コンテンツを復号する、前記サーバ装置の第1の暗号化手段に対応する第1の復号手段と、前記第1の復号手段で復号されたコンテンツを前記第3の復号手段で復号された利用条件データによって許諾された範囲で再生するための再生手段とを備える。

【0144】ここで、前期再生装置は、さらに、前記記録媒体装置の記録用媒体固有鍵記憶領域に格納された記録用媒体固有鍵をセキュアに取得する媒体固有鍵取得手段を備え、前記読み出し手段は、前記再暗号化タイトル鍵及び再暗号化利用条件データを前記記録媒体装置から読み出し、前記第3の復号手段は、前記読み出し手段で読み出した前記再暗号化タイトル鍵及び再暗号化利用条件データを前記媒体固有鍵で前記共通鍵暗号方式によって復号し、前記第1の復号手段は、前記暗号化コンテンツを、前記タイトル鍵を用いて前記共通鍵暗号方式によって復号し、前記再生手段は、前記利用条件データによって許諾された範囲で復号されたコンテンツを再生する。

【0145】ここで、前記再生装置及び前記記録媒体装置は、それぞれ、さらに第2の認証手段を備え、前記再生装置は、前記記録媒体装置から、前記媒体固有鍵を取得するのに先立って、もしくは、前記再生装置は、前記記録媒体装置によって、前記暗号化タイトル鍵及び暗号化利用条件データが読み出されるのに先立って、前記再生装置の第2の認証手段は、前記記録媒体装置を認証し、前記記録媒体装置の第2の認証手段は、前記再生装置の正当性を認証し、それぞれの認証が成功した場合に、前記再生装置は、前記記録媒体装置から、前記媒体固有鍵を取得する、もしくは、前記再生装置は、前記記録媒体装置によって、前記暗号化タイトル鍵及び暗号化利用条件データが読み出される。

【0146】ここで、前記利用条件データは、前記コンテンツの再生回数を制御する情報、もしくは、前記コンテンツの再生期間を制御する情報、もしくは、前記コンテンツの再生累積時間を制御する情報を含む。以上の説明から明らかなように、本発明による著作物保護システム、記録媒体装置、サーバ装置及び再生装置においては、暗号化タイトル鍵及び利用条件データの復号、及び再暗号化（暗号変換）を記録媒体装置の耐タンパモジュール部で行うことにより不正な第三者によるハッキングを困難にすることが可能となる。

【0147】また、記録媒体装置上での暗号変換やフォーマット変換を行う耐タンパモジュールを安全に更新することが可能となる以上、本発明に係わるデジタル著作物保護システムについて説明したが、本発明は、これらの実施の形態に限られないことは勿論である。次のように構成してもよい。

【0148】（1）上記の実施の形態では、暗号アルゴリズムとしてDES及び楕円暗号を利用する場合を説明

したが、これらに限定されない。他の暗号技術を適用してもよい。

（2）上記の実施の形態では、利用条件付き購入済みコンテンツについてメモリカードに保存する、又はメモリカードからコンテンツを再生する手順について述べたが、コンテンツが購入済みかどうかは、発明の本質ではない。例えば、利用条件データ付きのお試し版の無償コンテンツであっても同様の手順を実行することができる。

10 【0149】（3）上記の実施の形態では、メモリカードにコンテンツが保存されるものとしたが、記録媒体はメモリカードに限定されない。他の種類の記録媒体であってもよい。

（4）上記の実施の形態では、コンテンツを暗号化するものとしたが、コンテンツの一部を暗号化するものとしてもよい。

20 【0150】（5）上記の実施の形態では、コンテンツ毎に利用条件データが付加される場合について説明したがこれに限るものではない。例えば、利用条件データは、月単位で100個まで音楽データを購入するというようなものであってもかまわない。この場合、例えば、月極め契約を解除すると、利用条件判定部により、翌月から、メモリカードの記憶領域に格納されたコンテンツの再生を許可しないように構成してもよい。

【0151】（6）上記の実施の形態では、コンテンツ毎に利用条件データが付加される場合について説明したが、特に利用条件データが付加されない場合についても対応可能であることは言うまでもない。

30 （7）また、コンテンツ配信用サーバ装置は、メモリカードの配信用秘密鍵が暴露された場合に、配信用秘密鍵に対応する配信用公開鍵をリポークリストに登録し、リポークリストに登録された配信用公開鍵を用いてタイトル鍵等を暗号化してメモリカードに提供することを禁止する構成としてもよい。

【0152】（8）また、メモリカードの耐タンパモジュール部は、耐タンパ性のあるハードウェア、もしくは、耐タンパ性のあるソフトウェア、もしくは、両者の組み合わせで構成してもよい。

40 （9）また、配信データフォーマット又は記録データフォーマットの変更があった時に、メモリカードのデータフォーマット変換手段を構成する耐タンパモジュールを更新することで対応できるよう構成してもよい。

【0153】（10）また、コンテンツ配信サーバが利用する暗号方式（楕円暗号やDES暗号）の変更、あるいは、追加に対応して、メモリカードの耐タンパモジュール部で用いる暗号方式の変更あるいは追加が必要になった時に耐タンパモジュールを更新することで対応できるよう構成してもよい。

50 （11）上記（9）又は（10）において、メモリカードは、更新する耐タンパモジュールの正当性を判定する

耐タンパモジュール判定部を備え、耐タンパモジュール判定部が、耐タンパモジュールが正当と判定した場合に耐タンパモジュールを更新するよう構成してもよい。

【0154】(12) メモリカードは、予め複数の暗号方式を備えており、前記複数の暗号方式から一つが選択がされており、選択された暗号方式を用いて、暗号又は復号するように構成してもよい。

(13) メモリカードは、あらかじめ複数の配信秘密鍵を格納しておき、楕円復号手段においては、複数の配信秘密鍵から一つを選択利用するよう構成してもよい。

【0155】(14) 本実施の形態では、ヘッドホンステレオを用いた場合のデジタル著作物配信システムについて説明したが、これに限定されない。例えば、ヘッドホンステレオに代えて、携帯電話、Lモード対応の据え置き電話、携帯型情報端末装置、パーソナルコンピュータ、あるいは、インターネット接続機能を有するテレビ等の家電製品であっても構わない。これらの再生装置は、音楽、映画、電子書籍、ゲームプログラムなどのデジタル著作物を再生する。

【0156】また、コンテンツ配信用サーバ装置200とPC300とは、インターネット10を介して接続されているとしているが、この接続形態には限定されない。例えば、コンテンツ配信用サーバ装置とPC300とは、インターネット及び携帯電話網を介して接続されているとしてもよい。また、コンテンツ配信用サーバ装置には、放送装置が接続され、コンテンツなどの各種情報が放送波に乗せて放送され、テレビなどの家電製品は、放送波を受信し、受信した放送波から各種情報を抽出するとしてもよい。

【0157】(15) 上記の実施の形態では、コンテンツ配信用サーバとメモリカードとの間でチャレンジレスポンス型の相互の機器認証を行なうとしたが、他の方法を適用することもできる。

(16) 上記の実施の形態では、受信装置として、PCを用いる場合について説明したが、他の装置、例えば、携帯電話、KIOSK端末などとしてもできる。

【0158】(17) 上記の実施の形態では、利用条件データに施すハッシュ関数として、SHA-1を用いるが、他のハッシュ関数を用いることもできる。

(18) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【0159】また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、半導体メモリなど、に記録したもののとしてもよい。また、これらの記録媒体に記録されて

いる前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0160】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0161】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(19) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0162】

【発明の効果】以上説明したように、本発明は、送信装置から送信されたデジタル著作物を、受信装置を介して、可搬型の記録媒体装置に書き込み、再生装置により再生するデジタル著作物保護システムであって、前記デジタル著作物保護システムは、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報をネットワークを介して送信する前記送信装置を含み、ここで、前記記録媒体装置が前記受信装置に装着され、前記デジタル著作物保護システムは、さらに、ネットワークを介して前記第1暗号化情報を受信し、受信した前記第1暗号化情報を前記記録媒体装置へ出力する受信装置と、情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タンパモジュール部とを備える前記記録媒体装置とを含み、前記耐タンパモジュール部は、出力された前記第1暗号化情報を取得し、配信復号鍵に基づいて前記第1暗号化情報を復号して中間情報を生成し、前記記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第2暗号化情報を生成し、生成した第2暗号化情報を前記情報記憶領域に書き込み、ここで、前記第2暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、前記デジタル著作物保護システムは、さらに、前記情報記憶領域から前記第2暗号化情報を読み出し、前記媒体固有鍵をセキュアに読み出し、前記媒体固有鍵に基づいて前記第2暗号化情報を復号して復号コンテンツを生成し、生成した復号コンテンツを再生する前記再生装置を含む。

【0163】この構成によると、記録媒体装置の内部に有する耐タンパモジュール部により、暗号化された原コンテンツから構成される第1暗号化情報を復号しさらに暗号化するので、不正な第三者によるハッキングを困難

にすることができる。ここで、前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる前記配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した前記配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツと第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を送信し、前記受信装置は、前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を受信し、受信した前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を出力し、前記耐タンパモジュール部は、配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶しており、出力された前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を取得し、前記配信復号鍵を用いて、前記第 1 暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第 2 暗号化コンテンツ鍵を生成し、取得した前記暗号化コンテンツと生成した前記第 2 暗号化コンテンツ鍵とを含む前記第 2 暗号化情報を書き込み、前記再生装置は、前記記録媒体装置から前記媒体固有鍵をセキュアに取得し、前記情報記憶領域から、前記暗号化コンテンツと前記第 2 暗号化コンテンツ鍵とを含む前記第 2 暗号化情報を読み出し、取得した前記媒体固有鍵を用いて、前記第 2 暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する。

【0164】この構成によると、記録媒体装置において、コンテンツ鍵を配信復号鍵を用いて復号しさらに媒体固有鍵を用いて暗号化するのみであって、コンテンツを復号しさらに暗号化することはないので、記録媒体装置における処理の負荷を軽減することができる。また、本発明は、デジタル著作物を送信する送信装置と、ネットワークを介して受信した前記デジタル著作物を可搬型の記録媒体装置に記録する受信装置と、前記記録媒体装置に記録された前記デジタル著作物を再生する再生装置と、前記記録媒体装置とから構成されるデジタル著作物保護システムであって、前記送信装置は、デジタル著作物である原コンテンツと当該原コンテンツに固有の原コンテンツ鍵を予め記憶している記憶手段と、デジタル著作物の配信のために用いられる配信暗号鍵を取得する配信暗号鍵取得手段と、前記原コンテンツ鍵を用いて、前記原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成する暗号化手段と、前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を、ネットワークを介して、送信する送信手段

とを含み、ここで、前記記録媒体装置が前記受信装置に装着され、前記受信装置は、ネットワークを介して前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を受信する受信手段と、受信した前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を出力する出力手段とを含み、前記記録媒体装置は、情報を記憶するための領域を備えている情報記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを含み、前記耐タンパモジュール手段は、配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶している鍵記憶部と、出力された前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を取得する取得部と、前記配信復号鍵を用いて、前記第 1 暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成する復号部と、前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第 2 暗号化コンテンツ鍵を生成する暗号化部と、取得した前記暗号化コンテンツ及び生成した前記第 2 暗号化コンテンツ鍵を前記情報記憶手段に書き込む書込部とを含み、ここで、前記暗号化コンテンツ及び前記第 2 暗号化コンテンツ鍵が書き込まれた前記記録媒体装置が前記再生装置に装着され、前記再生装置は、前記鍵記憶部から前記媒体固有鍵をセキュアに取得する鍵取得手段と、前記情報記憶手段から前記暗号化コンテンツと前記第 2 暗号化コンテンツ鍵とを読み出す読出手段と、取得した前記媒体固有鍵を用いて、読み出した前記第 2 暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成するコンテンツ鍵復号手段と、生成された前記復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成するコンテンツ復号手段と、生成された復号コンテンツを再生する再生手段とを備える。

【0165】この構成によると、記録媒体装置の内部に有する耐タンパモジュール部により、復号し、再暗号化するので、不正な第三者によるハッキングを困難にし、また、暗号化コンテンツを復号し、さらに暗号化することはないので、記録媒体装置における処理の負荷を軽減することができる。また、本発明は、デジタル著作物をネットワークを介して送信する送信装置であって、前記デジタル著作物は、受信装置を介して、可搬型の記録媒体装置に書き込まれ、前記送信装置は、デジタル著作物である原コンテンツと当該原コンテンツに固有の原コンテンツ鍵を予め記憶している記憶手段と、デジタル著作物の配信のために用いられる配信暗号鍵を取得する配信暗号鍵取得手段と、前記原コンテンツ鍵を用いて、前記原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成する暗号化手段と、前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を、ネットワークを介して、送信する送信手段とを備える。

【0166】この構成によると、記録媒体装置の内部に

有する耐タンパモジュール部において、不正な第三者によるハッキングを困難にし、かつ記録媒体装置における処理の負荷を軽減することができるように、暗号化されたデジタル著作物を送信する送信装置を提供することができる。ここで、前記記憶手段は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記暗号化手段は、さらに、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第 1 暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第 1 暗号化利用条件情報を生成し、前記送信手段は、さらに、前記第 1 暗号化利用条件鍵及び前記第 1 暗号化利用条件情報を、ネットワークを介して、送信する。

【0167】この構成によると、コンテンツの利用条件を示す利用条件情報を送信するので、再生装置において、コンテンツの利用を制御することができる。ここで、前記配信暗号鍵取得手段は、公開鍵生成アルゴリズムを用いて生成された公開鍵である前記配信暗号鍵を取得し、前記暗号化手段は、公開鍵である配信暗号鍵を用いて、公開鍵暗号アルゴリズムにより、暗号化する。

【0168】この構成によると、公開鍵を用いて暗号化するので、鍵を安全に配布することができる。ここで、前記送信装置は、さらに、無効の配信暗号鍵を記録するための領域を備えるリポークリスト手段と、公開鍵である前記配信暗号鍵の生成において基にされた配信復号鍵が暴露された場合に、前記配信暗号鍵を前記リポークリスト手段に書き込む登録手段とを含み、ここで、前記送信装置は、新たにデジタル著作物であるコンテンツを送信し、前記配信鍵取得手段は、新たに配信暗号鍵を取得し、取得した配信暗号鍵がリポークリスト手段に書き込まれているか否かを判断し、書き込まれていると判断する場合には、前記暗号化手段に対して暗号化を禁止し、前記送信手段に対して送信を禁止する。

【0169】この構成によると、暴露された秘密鍵に対応する公開鍵の利用を制限するので、より安全にコンテンツを配布することができる。ここで、前記記憶手段は、さらに、前記デジタル著作物の利用条件を示す利用条件情報を記憶しており、前記送信手段は、さらに、前記記憶手段から前記利用条件情報を読み出し、読み出した前記利用条件情報にハッシュアルゴリズムを施してハッシュ値を生成し、生成した前記ハッシュ値と読み出した利用条件情報を、セキュアにネットワークを介して送信する。

【0170】この構成によると、配信経路において利用条件情報が改竄された場合に、前記利用条件情報に対応するデジタル著作物の利用を禁止することができる。ここで、前記送信装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証する認証手段を含み、前記配信暗号鍵取得手段は、前記認証に成功した場合にのみ、前記配信暗号鍵を前記記録媒体装置から取得し、前記暗号化手段は、前記認証に成功した場合にのみ、暗号化し、前記送信手段は、前記認証に成功した場合にのみ、送信する。

【0171】この構成によると、送信装置と記録媒体装置との間で相互に機器の正当性を認証するので、不正な機器に対してデジタル著作物を出力することを防止することができる。ここで、前記送信装置は、さらに、前記記録媒体装置が備える耐タンパモジュール部を更新するための更新情報を予め記憶している更新情報記憶手段と、前記更新情報記憶手段から前記更新情報を読み出し、読み出した前記更新情報を、ネットワーク及び受信装置を介して、前記記録媒体装置へ送信する更新情報送信手段とを含む。

【0172】この構成によると、耐タンパモジュールの更新用の情報を送信するので、記録媒体装置において、耐タンパモジュールを更新することができるようになる。ここで、前記送信装置は、さらに、前記更新情報記憶手段から前記更新情報を読み出し、読み出した更新情報にハッシュアルゴリズムを施してハッシュ値を生成し、生成したハッシュ値を、ネットワーク及び受信装置を介して、前記記録媒体装置へセキュアに送信するハッシュ手段を含む。

【0173】この構成によると、配信経路において耐タンパモジュールの更新用の情報が改竄された場合に、更新用の前記情報の利用を禁止することができる。ここで、前記更新情報記憶手段が記憶している更新情報は、前記耐タンパモジュール部が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含み、前記更新情報送信手段は、前記耐タンパモジュール部が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含む前記更新情報を読み出し、読み出した前記更新情報を送信する。

【0174】この構成によると、更新用の情報は、暗号化方式、復号方式又は変換方式を更新するための情報を含むので、耐タンパモジュール内の暗号化方式、復号方式又は変換方式を更新することができる。また、本発明は、送信装置から送信されたデジタル著作物を、受信装置を介して、記録する可搬型の記録媒体装置であって、前記記録媒体装置が前記受信装置に装着され、前記送信装置は、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第 1 暗号化情報を生成し、生成した第 1 暗号化情報を、ネットワークを介して、前記受信装置へ送信し、前記記録媒体装置は、情報を記憶するための領域を備える情報記憶手段と、耐タンパ性を有する耐タンパモジュール手段とを備え、前記耐タンパモジュール手段は、配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶している鍵記憶部と、前記受信

装置を介して、送信された前記第 1 暗号化情報を取得する取得部と、前記配信復号鍵に基づいて前記第 1 暗号化情報を復号して中間情報を生成する復号部と、前記媒体固有鍵に基づいて前記中間情報を暗号化して第 2 暗号化情報を生成する暗号化部と、生成した第 2 暗号化情報を前記情報記憶手段に書き込む書込部とを備える。

【0175】この構成によると、不正な第三者によるハッキングを困難にする記録媒体装置を提供することができる。ここで、前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ及び第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を送信し、前記取得部は、出力された前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を含む前記第 1 暗号化情報を取得し、前記復号部は、前記配信復号鍵を用いて、前記第 1 暗号化情報に含まれる前記第 1 暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記第 1 暗号化情報に含まれる前記暗号化コンテンツ及び生成した前記中間コンテンツ鍵を含む前記中間情報を生成し、前記暗号化部は、前記媒体固有鍵を用いて、前記中間情報に含まれる前記中間コンテンツ鍵を暗号化して第 2 暗号化コンテンツ鍵を生成し、前記中間情報に含まれる前記暗号化コンテンツ及び生成した前記第 2 暗号化コンテンツ鍵を含む前記第 2 暗号化情報を書き込む。

【0176】この構成によると、記録媒体装置において、コンテンツ鍵を配信復号鍵を用いて復号しさらに媒体固有鍵を用いて暗号化するのみであって、コンテンツを復号しさらに暗号化することはないので、記録媒体装置における処理の負荷を軽減することができる。ここで、前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第 1 暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第 1 暗号化利用条件情報を生成し、前記第 1 暗号化利用条件鍵及び前記第 1 暗号化利用条件情報を、ネットワークを介して、前記受信装置へ送信し、前記取得部は、さらに、前記受信装置を介して、前記第 1 暗号化利用条件鍵及び前記第 1 暗号化利用条件情報を取得し、前記復号部は、さらに、前記配信復号鍵を用いて、前記第 1 暗号化利用条件鍵を復号して中間利用条件鍵を生成し、生成した前記中間利用条件鍵を用いて、前記第 1 暗号化利用条件情報を復号して、中間利用

条件情報を生成し、前記暗号化部は、さらに、前記媒体固有鍵を用いて、前記中間利用条件情報を暗号化して第 2 暗号化利用条件情報を生成し、前記書込部は、さらに、生成した第 2 暗号化利用条件情報を前記情報記憶手段に書き込む。

【0177】この構成によると、コンテンツの利用条件を示す利用条件情報を記憶するので、再生装置において、コンテンツの利用を制御することができる。ここで、前記送信装置は、さらに、秘密鍵である配信復号鍵を基にして公開鍵生成アルゴリズムを用いて生成された公開鍵である前記配信暗号鍵を取得し、公開鍵である配信暗号鍵を用いて、公開鍵暗号アルゴリズムにより、暗号化し、前記復号部は、公開鍵復号アルゴリズムにより、前記配信復号鍵を用いて復号する。

【0178】この構成によると、公開鍵を用いて暗号化し、秘密鍵を用いて復号するので、鍵を安全に配布することができる。ここで、前記耐タンパモジュール手段は、さらに、前記復号部により生成された配信データ形式である前記中間情報を変換して、記録データ形式の記録中間情報を生成する変換部を含み、前記暗号化部は、前記中間情報に代えて、前記記録中間情報を暗号化する。

【0179】この構成によると、配信用のデータ形式を記録用のデータ形式に変換するので、配信用のデータ形式と記録用のデータ形式が異なっている場合に対応できる。また、新たにデータ形式が追加された場合であっても、容易に対応することができる。ここで、前記送信装置は、前記記録媒体装置が備える前記耐タンパモジュール手段を更新するための更新情報を予め記憶しており、前記更新情報を読み出し、読み出した前記更新情報を、ネットワーク及び受信装置を介して、前記記録媒体装置へ送信し、前記耐タンパモジュール手段は、マイクロプロセッサとコンピュータプログラムを記録している半導体メモリを含み、前記コンピュータプログラムに従って、前記マイクロプロセッサが動作することにより、前記耐タンパモジュール手段に含まれる構成要素が動作し、前記取得部は、前記受信装置を介して、前記更新情報を取得し、前記耐タンパモジュール手段は、さらに、取得した前記更新情報を用いて、前記コンピュータプログラムを更新し、これにより、前記耐タンパモジュール手段に含まれる構成要素が更新される更新部を含む。

【0180】この構成によると、耐タンパモジュールの更新用の情報を取得して、記録媒体装置において、耐タンパモジュールを更新することができるようになる。ここで、前記送信装置は、さらに、前記更新情報を読み出し、読み出した更新情報にハッシュアルゴリズムを施して第 1 ハッシュ値を生成し、生成した第 1 ハッシュ値を、ネットワーク及び受信装置を介して、前記記録媒体装置へセキュアに送信し、前記耐タンパモジュール手段は、さらに、取得した前記更新情報に前記ハッシュアル

ゴリズムを施して第2ハッシュ値を生成するハッシュ部と、取得した前記第1ハッシュ値と生成した前記第2ハッシュ値とが一致するか否かを判断する比較判断部とを含み、前記更新部は、前記比較判断部により一致すると判断された場合にのみ、更新する。

【0181】この構成によると、配信経路において耐タンパモジュールの更新用の情報が改竄された場合に、更新用の前記情報の利用を禁止することができる。ここで、前記送信装置が記憶している更新情報は、前記耐タンパモジュール手段が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含み、前記前記更新情報を送信し、前記取得部は、暗号化方式、復号方式、又はデータ変換方式を更新するための前記更新情報を前記受信装置を介して取得し、前記更新部は、取得した前記更新情報を用いて、前記コンピュータプログラムを更新し、これにより、前記耐タンパモジュール手段に含まれる暗号化部、復号部、又は変換部が更新される。

【0182】この構成によると、更新用の情報は、暗号化方式、復号方式又は変換方式を更新するための情報を含むので、耐タンパモジュール内の暗号化方式、復号方式又は変換方式を更新することができる。ここで、前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報を記憶しており、前記利用条件情報を読み出し、読み出した前記利用条件情報にハッシュアルゴリズムを施して第1ハッシュ値を生成し、生成した前記第1ハッシュ値と読み出した利用条件情報を、ネットワークを介してセキュアに送信し、前記取得部は、さらに、前記受信装置を介して、送信された前記第1ハッシュ値と前記利用条件情報とを取得し、前記耐タンパモジュール手段は、さらに、取得した前記利用条件情報に前記ハッシュアルゴリズムを施して第2ハッシュ値を生成するハッシュ部と、取得した前記第1ハッシュ値と生成した前記第2ハッシュ値とが一致するか否かを判断する比較判断部とを含み、前記暗号化部は、前記比較判断部により一致すると判断された場合にのみ、暗号化し、前記書込部は、前記比較判断部により一致すると判断された場合にのみ、書き込む。

【0183】この構成によると、配信経路において利用条件情報が改竄された場合に、前記利用条件情報に対応するデジタル著作物の利用を禁止することができる。ここで、前記送信装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証し、前記認証に成功した場合にのみ、前記配信暗号鍵を前記記録媒体装置から取得し、暗号化し、送信し、前記耐タンパモジュール手段は、さらに、前記送信装置との間で相互に機器の正当性を認証する認証手段を含み、前記取得部は、前記認証に成功した場合にのみ、取得し、前記復号部は、前記認証に成功した場合にのみ、復号し、前記暗号化部は、前記

前記認証に成功した場合にのみ、書き込む。

【0184】この構成によると、送信装置と記録媒体装置との間で相互に機器の正当性を認証するので、不正な装置からデジタル著作物を取得することを防止することができる。ここで、前記記録媒体装置は、再生装置に装着され、前記再生装置は、前記情報記憶手段から情報を読み出し、前記耐タンパモジュール手段は、さらに、前記再生装置との間で相互に機器の正当性を認証し、前記認証に成功した場合にのみ、前記再生装置に対して情報の読み出しを許可する認証手段を含む。

【0185】この構成によると、記録媒体装置と再生装置との間で相互に機器の正当性を認証するので、不正な装置へデジタル著作物を出力することを防止することができる。ここで、前記復号部は、複数の復号方式を予め備えており、前記複数の復号方式から選択した1個の復号方式を用いて、復号し、ここで、選択した前記復号方式は、前記送信装置で用いられる暗号化方式の逆変換を行う。また、前記暗号化部は、複数の暗号化方式を予め備えており、前記複数の暗号化方式から選択した1個の暗号方式を用いて、暗号化する。

【0186】この構成によると、記録媒体装置は、複数の復号方式から又は複数の暗号方式から1個を選択して用いるので、送信装置又は再生装置が有する方式に合わせて、変更が容易である。ここで、前記鍵記憶部は、複数の配信復号鍵候補を記憶しており、前記複数の配信復号鍵候補から1個の配信復号鍵候補が前記配信復号鍵として選択されており、前記復号部は、選択された前記配信復号鍵を用いる。

【0187】この構成によると、記録媒体装置は、複数の配信用秘密鍵から1個を選択して用いるので、選択された配信用秘密鍵が暴露された場合であっても、他の配信用秘密鍵を使用することにより、継続して記録媒体装置を利用することができる。ここで、前記耐タンパモジュール手段は、ソフトウェア、ハードウェア、又はソフトウェア及びハードウェアの組合せにより、耐タンパ性を実現している。

【0188】この構成によると、耐タンパモジュールへの不正なアタックに対して防御が可能である。ここで、送信装置からネットワーク及び受信装置を介して送信されて可搬型の記録媒体装置に書き込まれたデジタル著作物を再生する再生装置であって、前記記録媒体装置が前記受信装置に装着され、前記送信装置は、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報をネットワークを介して前記受信装置へ送信し、前記記録媒体装置は、情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タンパモジュール部とを備え、前記耐タンパモジュール部は、前記受信装置を介して送信された前記第1暗号化情報を取得し、配信復号鍵に基づいて前記第1暗号化情報を復号して中間情報を生成し、前

記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第2暗号化情報を生成し、生成した第2暗号化情報を前記情報記憶領域に書き込み、ここで、前記第2暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、前記再生装置は、前記記録媒体装置から前記媒体固有鍵をセキュアに取得する鍵取得手段と、前記情報記憶領域から前記第2暗号化情報を読み出す読出手段と、取得した前記媒体固有鍵に基づいて、読み出した前記第2暗号化を復号して、復号コンテンツを生成する復号手段と、生成された復号コンテンツを再生する再生手段とを備える。

【0189】この構成によると、不正な第三者によるハッキングを困難にする記録媒体装置に記録されているデジタル著作物を再生することができる。ここで、前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第1暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツと第1暗号化コンテンツ鍵とを含む前記第1暗号化情報を送信し、前記耐タンパモジュール部は、前記配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶しており、出力された前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を含む前記第1暗号化情報を取得し、前記配信復号鍵を用いて、前記第1暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第2暗号化コンテンツ鍵を生成し、取得した前記暗号化コンテンツと生成した前記第2暗号化コンテンツ鍵とを含む前記第2暗号化情報を書き込み、前記読出手段は、前記暗号化コンテンツと前記第2暗号化コンテンツ鍵とを含む前記第2暗号化情報を読み出し、前記復号手段は、取得した前記媒体固有鍵を用いて、読み出した前記第2暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する。

【0190】この構成によると、記録媒体装置において、コンテンツ鍵を配信復号鍵を用いて復号しさらに媒体固有鍵を用いて暗号化するのみであって、コンテンツを復号しさらに暗号化することはないので、記録媒体装置における処理の負荷を軽減することができる。ここで、前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第1暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第1暗号化利用条件情報を生成し、

前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を、ネットワークを介して、前記受信装置へ送信し、前記記録媒体装置は、さらに、前記受信装置を介して、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を取得し、前記配信復号鍵を用いて、前記第1暗号化利用条件鍵を復号して中間利用条件鍵を生成し、生成した前記中間利用条件鍵を用いて、前記第1暗号化利用条件情報を復号して、中間利用条件情報を生成し、前記媒体固有鍵を用いて、前記中間利用条件情報を暗号化して第2暗号化利用条件情報を生成し、生成した第2暗号化利用条件情報を前記情報記憶領域に書き込み、前記読出手段は、さらに、前記情報記憶領域から前記第2暗号化利用条件情報を読み出し、前記復号手段は、さらに、前記媒体固有鍵に基づいて、読み出した前記第2暗号化利用条件情報を復号して復号利用条件情報を生成し、前記再生手段は、さらに、生成された復号利用条件情報に基づいて復号コンテンツの再生の可否を判断し、再生可と判断される場合にのみ、前記生成された復号コンテンツを再生する。

【0191】この構成によると、取得した利用条件情報に基づいて、コンテンツの利用を制御できる。ここで、前記利用条件情報は、前記復号コンテンツの再生回数を制限する情報、前記復号コンテンツの再生期間を制限する情報、又は前記復号コンテンツの再生累積時間を制限する情報を含み、前記再生手段は、再生回数を制限する情報、再生期間を制限する情報、又は再生累積時間を制御する情報に基づいて復号コンテンツの再生の可否を判断する。

【0192】この構成によると、前記復号コンテンツの再生回数を制限する情報、前記復号コンテンツの再生期間を制限する情報、又は前記復号コンテンツの再生累積時間を制限する情報に基づいて、コンテンツの再生の可否を判断できる。ここで、前記再生装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証する認証手段を含み、前記鍵取得手段は、前記認証に成功した場合にのみ、取得し、前記読出手段は、前記認証に成功した場合にのみ、読み出す。

【0193】この構成によると、再生装置と記録媒体装置との間で相互に機器の正当性を認証するので、不正な装置からデジタル著作物を取得することを防止できる。

【図面の簡単な説明】

【図1】デジタル著作物保護システム100の構成を示すブロック図である。

【図2】コンテンツ配信用サーバ装置200及びメモリカード400の構成を示すブロック図である。

【図3】メモリカード400の構成を示すブロック図である。

【図4】PC300の構成を示すブロック図である

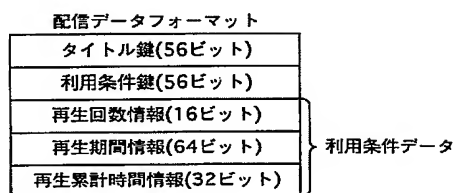
【図5】メモリカード400及びヘッドホンステレオ500の構成を示すブロック図である。

【図6】配信データフォーマットの構成を示す。
 【図7】記録データフォーマットの構成を示す。
 【図8】メモリカード400への書き込み時の動作を示すフローチャートである。図9へ続く。
 【図9】メモリカード400への書き込み時の動作を示すフローチャートである。図10へ続く。
 【図10】メモリカード400への書き込み時の動作を示すフローチャートである。図9から続く。
 【図11】メモリカード400からの読み出し時の動作を示すフローチャートである。図12へ続く。
 【図12】メモリカード400からの読み出し時の動作を示すフローチャートである。図11から続く。
 【図13】コンテンツ配信用サーバ装置200b及びメモリカード400bの構成を示すブロック図である。
 【図14】メモリカード400bの構成を示すブロック図である。
 【図15】メモリカード400b及びヘッドホンステレオ500の構成を示すブロック図である。
 【図16】配信データフォーマットの構成を示す。
 【図17】記録データフォーマットの構成を示す。
 【図18】メモリカード400bへの書き込み時の動作を示すフローチャートである。図19へ続く。
 【図19】メモリカード400bへの書き込み時の動作を示すフローチャートである。図20へ続く。
 【図20】メモリカード400bへの書き込み時の動作を示すフローチャートである。図19から続く。
 【図21】コンテンツ配信用サーバ装置200c及びメモリカード400cの構成を示すブロック図である。
 【図22】デジタル著作物保護システム100cにおいて、メモリカード400c内の耐タンパモジュール部410cに含まれるコンピュータ又はデータを更新する場合の動作を示すフローチャートである。

【符号の説明】

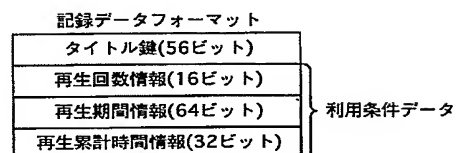
10 インターネット
 100 デジタル著作物保護システム
 200 コンテンツ配信用サーバ装置
 201 コンテンツ格納部
 202 配信データ格納部

【図6】

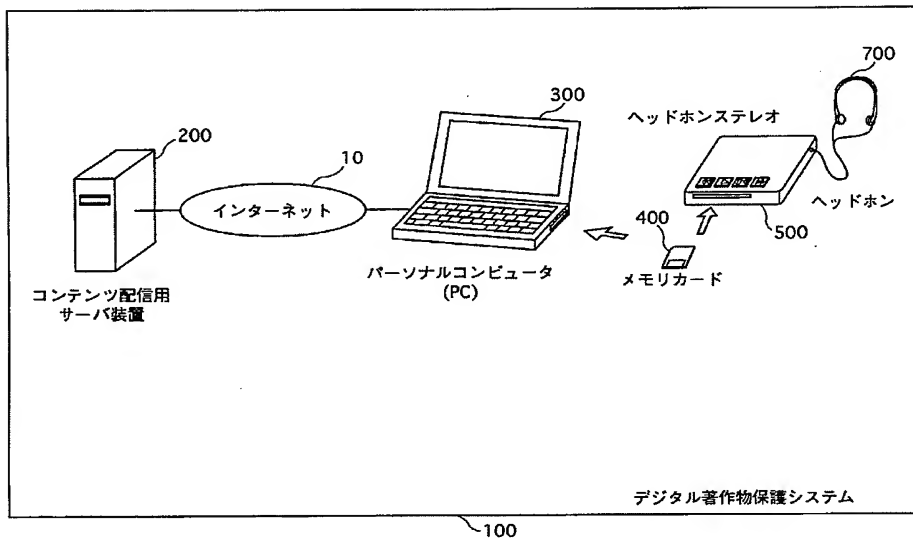


211 第1認証部
 212 配信公開鍵取得部
 214 楕円暗号化部
 215 DES暗号化部
 250 DES暗号化部
 300 PC
 301 マイクロプロセッサ
 302 メモリ部
 303 入力部
 304 表示部
 305 通信部
 306 メモリカード接続部
 400 メモリカード
 410 耐タンパモジュール部
 411 第1認証部
 412 配信公開鍵格納部
 413 配信秘密鍵格納部
 414 楕円復号部
 415 DES復号部
 416 変換部
 417 第2認証部
 418 記録媒体鍵格納部
 419 DES暗号化部
 422 記録データ格納部
 423 配信データ格納部
 430 情報記憶部
 431 第2記憶領域
 432 第1記憶領域
 500 ヘッドホンステレオ
 517 第2認証部
 518 記録媒体鍵取得部
 519 DES復号部
 531 再暗号化データ取得部
 532 記録データ格納部
 540 利用条件判定部
 541 再生部
 550 DES復号部
 700 ヘッドホン

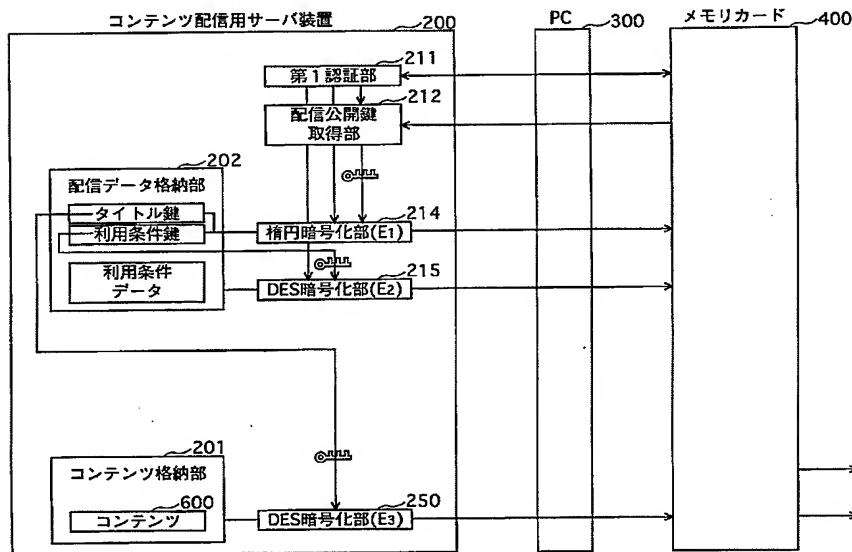
【図7】



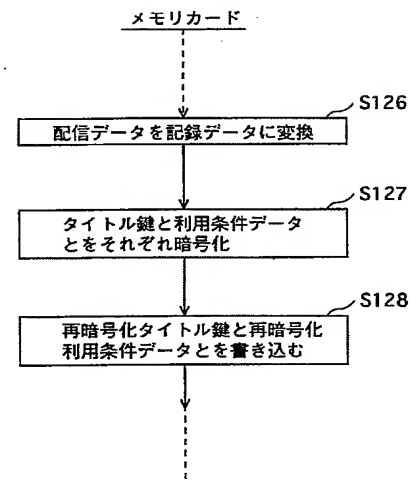
【図1】



【図2】



【図10】



【図16】

配信データフォーマット	
タイトル鍵(56ビット)	
ダイジェスト(64ビット)	
再生回数情報(16ビット)	
再生期間情報(64ビット)	
再生累計時間情報(32ビット)	

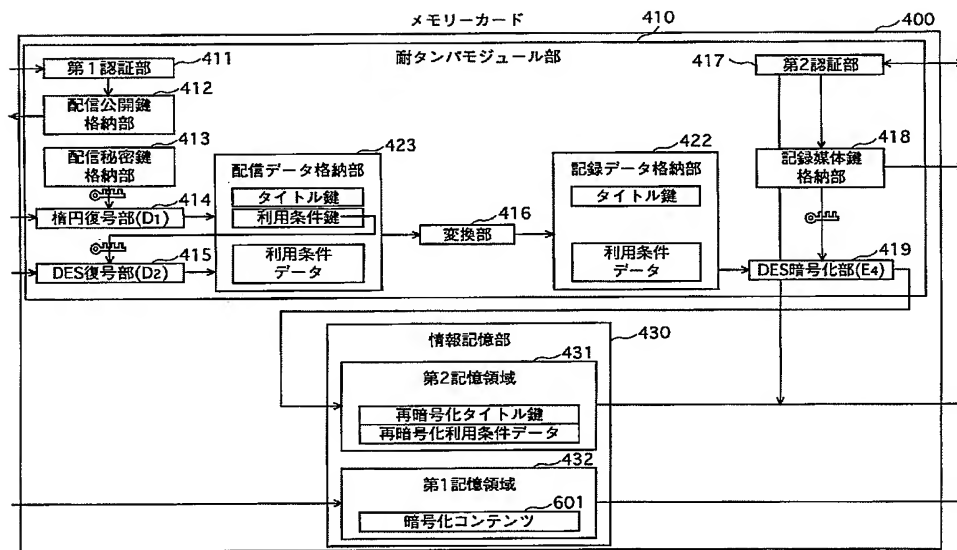
【図17】

記録データフォーマット	
タイトル鍵(56ビット)	
再生回数情報(16ビット)	
再生期間情報(64ビット)	
再生累計時間情報(32ビット)	

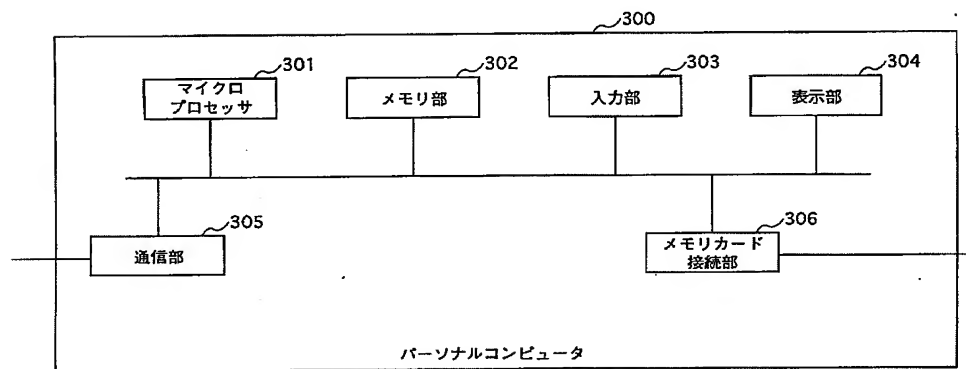
利用条件データ

利用条件データ

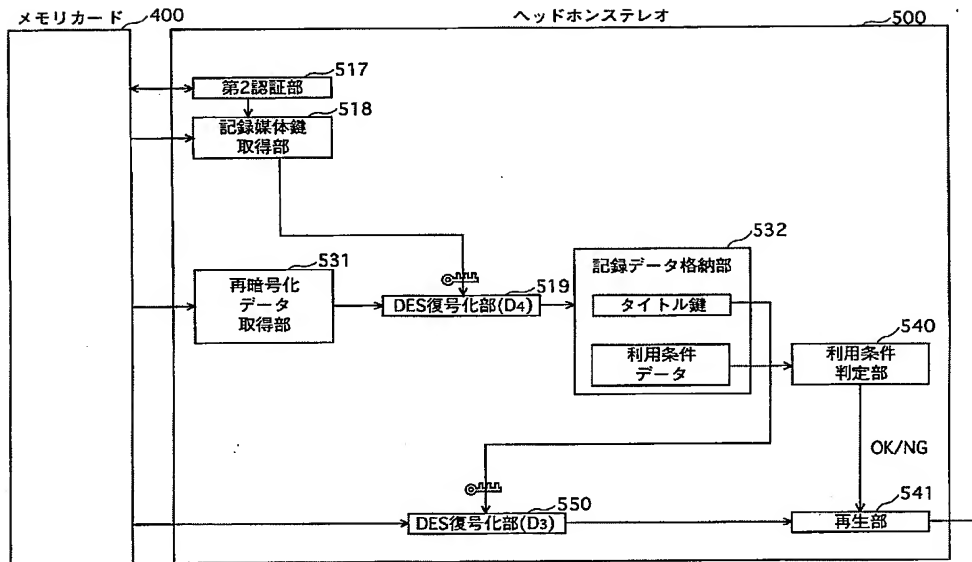
【図3】



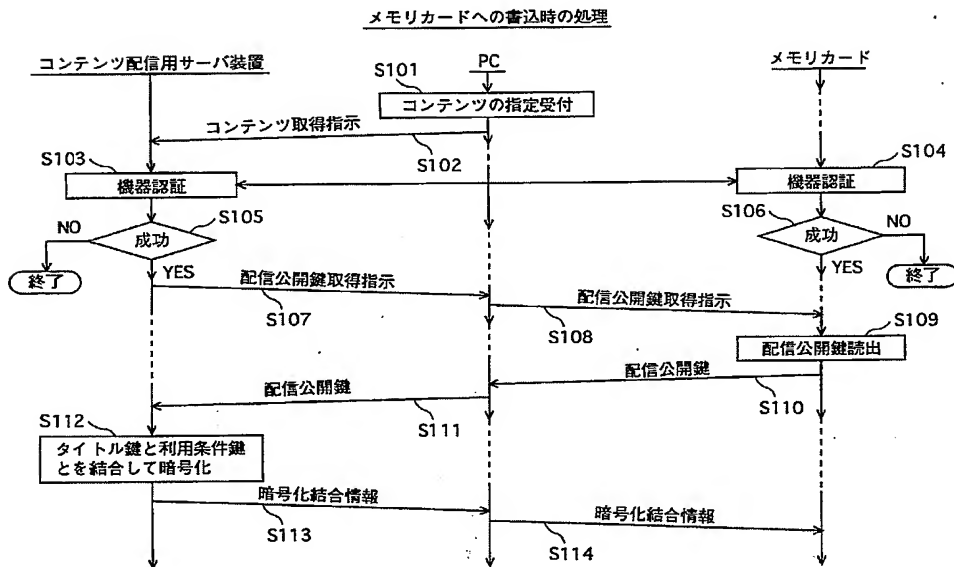
【図4】



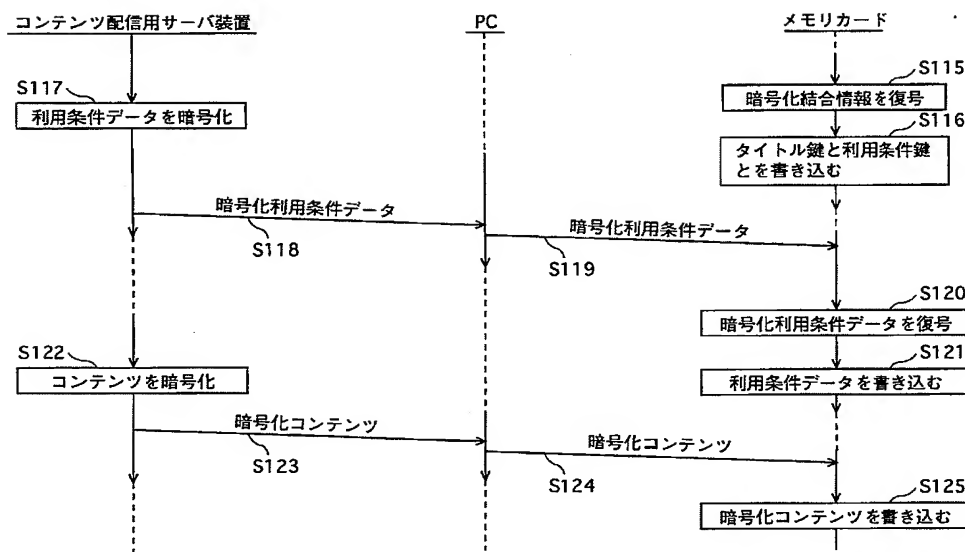
【図5】



【図8】

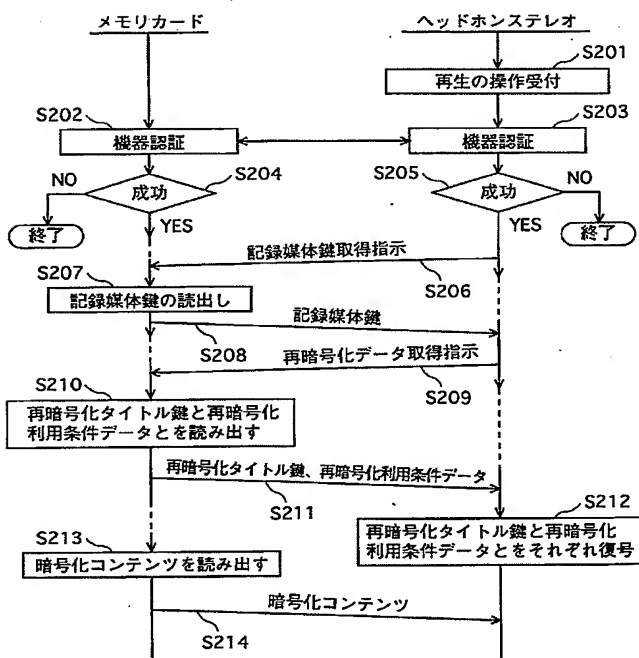


【図 9】

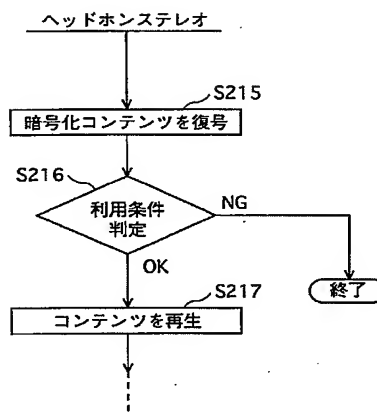


【図 11】

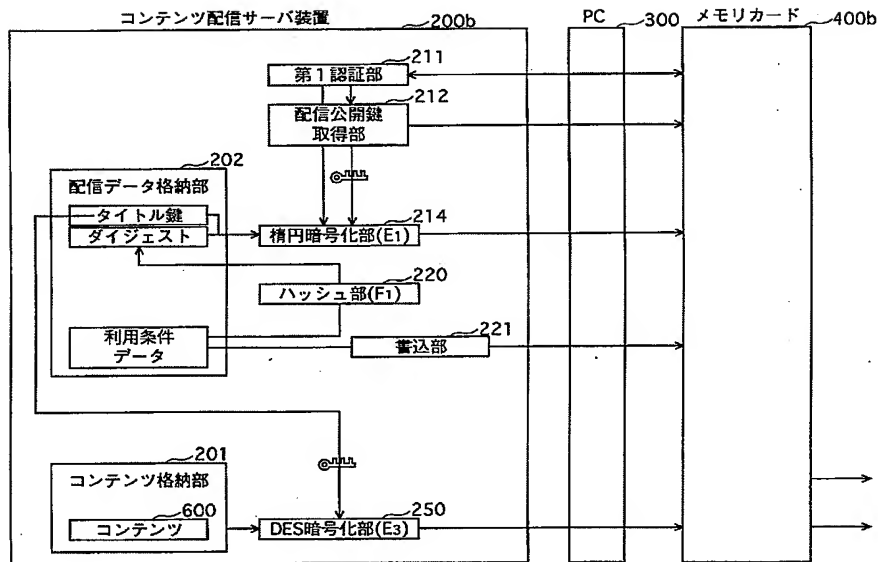
メモリカードからの読出し時の処理



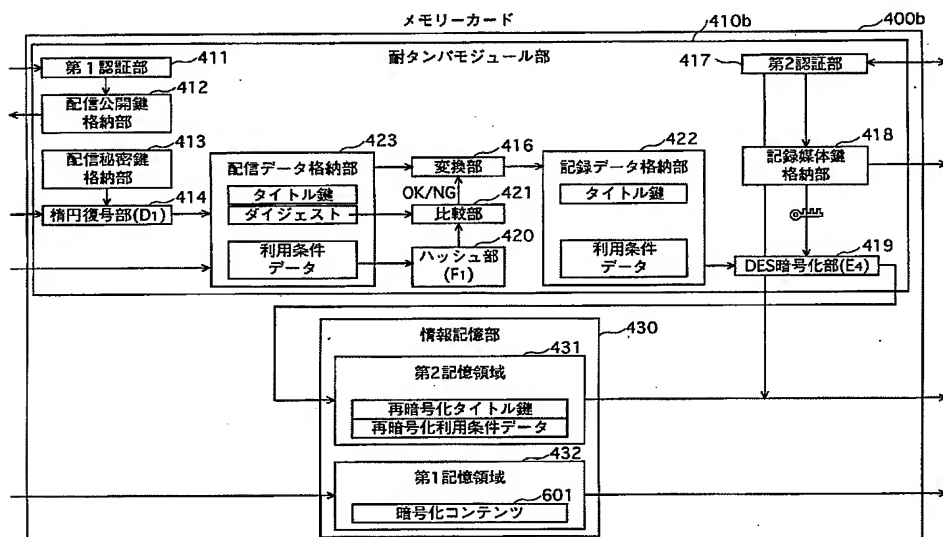
【図 12】



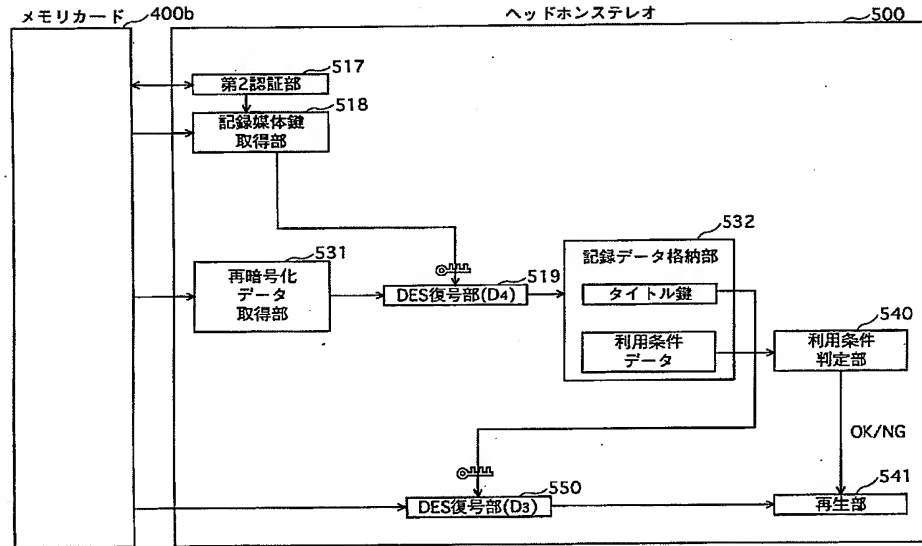
【図13】



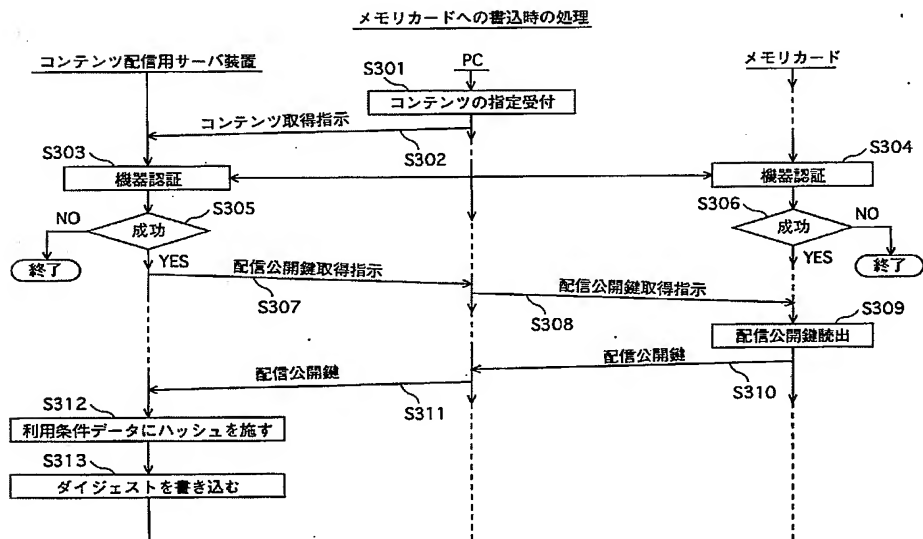
【図14】



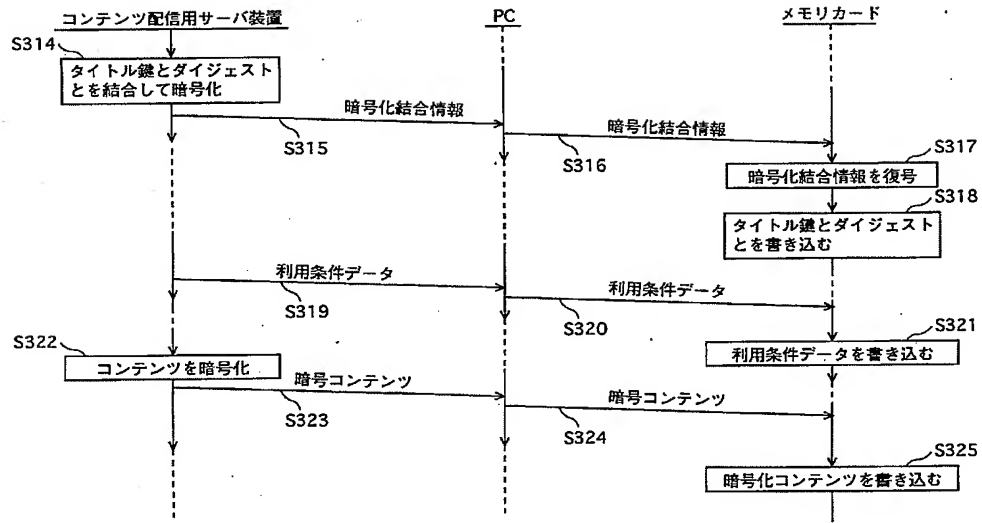
【図15】



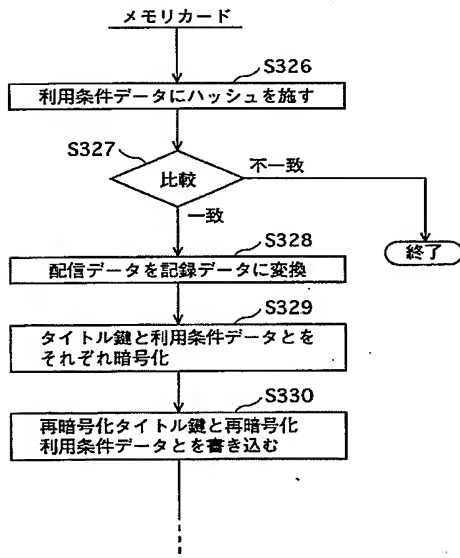
【図18】



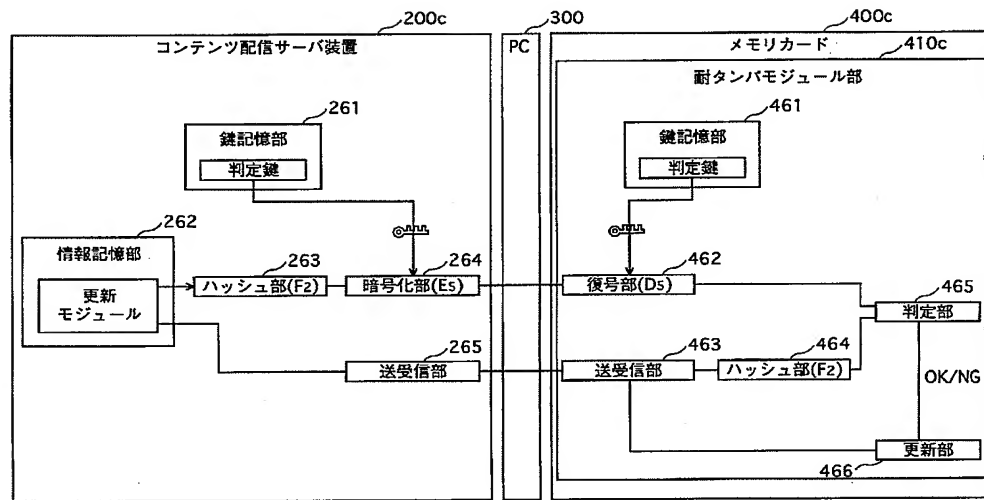
【図19】



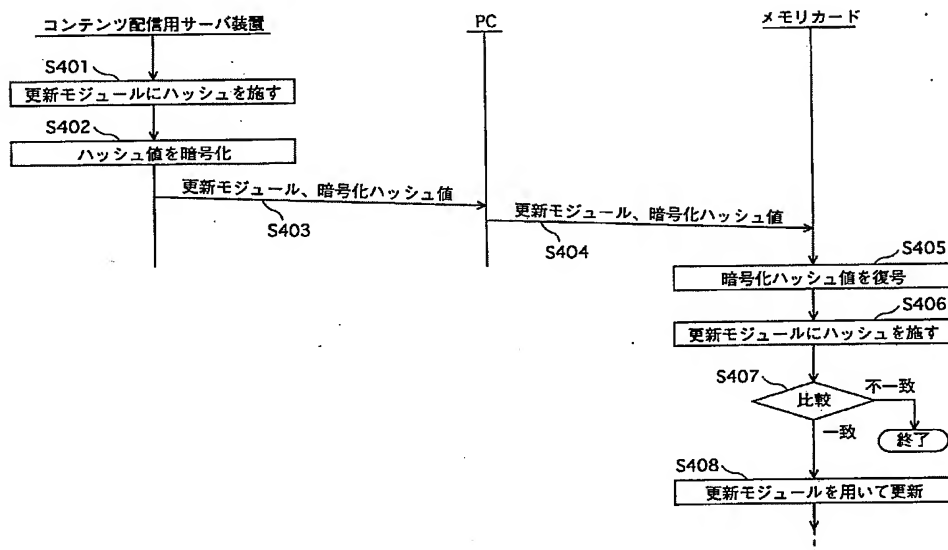
【図20】



【図 21】



【図 22】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
G 0 6 K 19/00		G 1 1 B 20/10	D 5 J 1 0 4
			H
G 0 9 C 1/00	6 6 0	H 0 4 L 9/00	6 0 1 A
G 1 1 B 20/10			6 0 1 B
		G 0 6 K 19/00	Q
H 0 4 N 5/765			R
5/91		H 0 4 N 5/91	L

5/93

P
Z

5/93

(72) 発明者 宮▲ざき▼ 雅也
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 関部 勉
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 中西 良明
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 松崎 なつめ
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

F ターム (参考) 5B017 AA06 BA07 CA16
5B035 AA13 BB09 BB11 BC00 CA11
CA29

5B058 CA02 CA23 KA01 KA04 KA06
KA12 KA31 KA35 YA20

5C053 FA13 GB06 JA21 LA11 LA14

5D044 BC01 BC04 CC04 DE17 DE50
GK17 HL08

5J104 AA01 AA12 AA16 AA34 EA04
EA19 EA22 JA03 JA21 JA31
KA04 KA05 KA06 NA02 NA12
NA35 NA40 NA41 NA42 PA14

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成17年9月29日(2005.9.29)

【公開番号】特開2003-158514(P2003-158514A)

【公開日】平成15年5月30日(2003.5.30)

【出願番号】特願2002-199142(P2002-199142)

【国際特許分類第7版】

H 0 4 L 9/08
 G 0 6 F 12/14
 G 0 6 K 17/00
 G 0 6 K 19/00
 G 0 6 K 19/10
 G 0 9 C 1/00
 G 1 1 B 20/10
 H 0 4 N 5/765
 H 0 4 N 5/91
 H 0 4 N 5/93

【F I】

H 0 4 L	9/00	6 0 1 A
G 0 6 F	12/14	3 2 0 B
G 0 6 K	17/00	D
G 0 6 K	17/00	L
G 0 6 K	17/00	T
G 0 9 C	1/00	6 6 0 A
G 1 1 B	20/10	D
G 1 1 B	20/10	H
H 0 4 L	9/00	6 0 1 B
G 0 6 K	19/00	Q
G 0 6 K	19/00	R
H 0 4 N	5/91	L
H 0 4 N	5/91	P
H 0 4 N	5/93	Z

【手続補正書】

【提出日】平成17年4月21日(2005.4.21)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正の内容】

【発明の名称】デジタル情報保護システム、記録媒体装置、送信装置及び再生装置

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

送信装置から送信されたデジタル情報を、受信装置を介して、可搬型の記録媒体装置に

書き込み、再生装置により再生するデジタル情報保護システムであって、

前記デジタル情報保護システムは、デジタル情報を配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報をネットワークを介して送信する前記送信装置を含み、

ここで、前記記録媒体装置が前記受信装置に装着され、

前記デジタル情報保護システムは、さらに、

ネットワークを介して前記第1暗号化情報を受信し、受信した前記第1暗号化情報を前記記録媒体装置へ出力する受信装置と、

情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タンパモジュール部とを備える前記記録媒体装置とを含み、

前記耐タンパモジュール部は、出力された前記第1暗号化情報を取得し、配信復号鍵に基づいて前記第1暗号化情報を復号して中間情報を生成し、前記記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第2暗号化情報を生成し、生成した第2暗号化情報を前記情報記憶領域に書き込み、

ここで、前記第2暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、

前記デジタル情報保護システムは、さらに、前記情報記憶領域から前記第2暗号化情報を読み出し、前記媒体固有鍵をセキュアに読み出し、前記媒体固有鍵に基づいて前記第2暗号化情報を復号して復号デジタル情報を生成し、生成した復号デジタル情報を再生する前記再生装置を含む

ことを特徴とするデジタル情報保護システム。

【請求項2】

前記送信装置は、前記デジタル情報として、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報を、ネットワークを介して、前記受信装置へ送信し、

前記記録媒体装置は、前記受信装置を介して、前記第1暗号化情報を取得することを特徴とする請求項1に記載のデジタル情報保護システム。

【請求項3】

前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる前記配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した前記配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第1暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツと第1暗号化コンテンツ鍵とを含む前記第1暗号化情報を送信し、

前記受信装置は、前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を含む前記第1暗号化情報を受信し、受信した前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を出力し、

前記耐タンパモジュール部は、配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶しており、出力された前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を含む前記第1暗号化情報を取得し、前記配信復号鍵を用いて、前記第1暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第2暗号化コンテンツ鍵を生成し、取得した前記暗号化コンテンツと生成した前記第2暗号化コンテンツ鍵とを含む前記第2暗号化情報を書き込み、

前記再生装置は、前記記録媒体装置から前記媒体固有鍵をセキュアに取得し、前記情報記憶領域から、前記暗号化コンテンツと前記第2暗号化コンテンツ鍵とを含む前記第2暗号化情報を読み出し、取得した前記媒体固有鍵を用いて、前記第2暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する

ことを特徴とする請求項2に記載のデジタル情報保護システム。

【請求項4】

前記送信装置は、前記デジタル情報として、コンテンツ鍵と利用条件の少なくとも一方を配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報を、ネットワークを介して、前記受信装置へ送信し、

前記記録媒体装置は、前記受信装置を介して、前記第1暗号化情報を取得することを特徴とする請求項1に記載のデジタル情報保護システム。

【請求項5】

デジタル著作物を送信する送信装置と、ネットワークを介して受信した前記デジタル著作物を可搬型の記録媒体装置に記録する受信装置と、前記記録媒体装置に記録された前記デジタル著作物を再生する再生装置と、前記記録媒体装置とから構成されるデジタル情報保護システムであって、

前記送信装置は、

デジタル著作物である原コンテンツと当該原コンテンツに固有の原コンテンツ鍵を予め記憶している記憶手段と、

デジタル著作物の配信のために用いられる配信暗号鍵を取得する配信暗号鍵取得手段と

、
前記原コンテンツ鍵を用いて、前記原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第1暗号化コンテンツ鍵を生成する暗号化手段と、

前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を、ネットワークを介して、送信する送信手段とを含み、

ここで、前記記録媒体装置が前記受信装置に装着され、

前記受信装置は、

ネットワークを介して前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を受信する受信手段と、

受信した前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を出力する出力手段とを含み、

前記記録媒体装置は、

情報を記憶するための領域を備えている情報記憶手段と、

耐タンパ性を有する耐タンパモジュール手段とを含み、

前記耐タンパモジュール手段は、

配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶している鍵記憶部と、

出力された前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を取得する取得部と

、
前記配信復号鍵を用いて、前記第1暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成する復号部と、

前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第2暗号化コンテンツ鍵を生成する暗号化部と、

取得した前記暗号化コンテンツ及び生成した前記第2暗号化コンテンツ鍵を前記情報記憶手段に書き込む書込部とを含み、

ここで、前記暗号化コンテンツ及び前記第2暗号化コンテンツ鍵が書き込まれた前記記録媒体装置が前記再生装置に装着され、

前記再生装置は、

前記鍵記憶部から前記媒体固有鍵をセキュアに取得する鍵取得手段と、

前記情報記憶手段から前記暗号化コンテンツと前記第2暗号化コンテンツ鍵とを読み出す読出手段と、

取得した前記媒体固有鍵を用いて、読み出した前記第2暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成するコンテンツ鍵復号手段と、

生成された前記復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成するコンテンツ復号手段と、

生成された復号コンテンツを再生する再生手段とを備える

ことを特徴とするデジタル情報保護システム。

【請求項 6】

デジタル著作物をネットワークを介して送信する送信装置であって、
前記デジタル著作物は、受信装置を介して、可搬型の記録媒体装置に書き込まれ、
前記送信装置は、
デジタル著作物である原コンテンツと当該原コンテンツに固有の原コンテンツ鍵を予め記憶している記憶手段と、
デジタル著作物の配信のために用いられる配信暗号鍵を取得する配信暗号鍵取得手段と

、
前記原コンテンツ鍵を用いて、前記原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第 1 暗号化コンテンツ鍵を生成する暗号化手段と、

前記暗号化コンテンツ及び前記第 1 暗号化コンテンツ鍵を、ネットワークを介して、送信する送信手段とを備え、

前記記憶手段は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、

前記暗号化手段は、さらに、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第 1 暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第 1 暗号化利用条件情報を生成し、

前記送信手段は、さらに、前記第 1 暗号化利用条件鍵及び前記第 1 暗号化利用条件情報を、ネットワークを介して、送信する

ことを特徴とする送信装置。

【請求項 7】

前記配信暗号鍵取得手段は、公開鍵生成アルゴリズムを用いて生成された公開鍵である前記配信暗号鍵を取得し、

前記暗号化手段は、公開鍵である配信暗号鍵を用いて、公開鍵暗号アルゴリズムにより、暗号化する。

ことを特徴とする請求項 6 に記載の送信装置。

【請求項 8】

前記送信装置は、さらに、

無効の配信暗号鍵を記録するための領域を備えるリポークリスト手段と、

公開鍵である前記配信暗号鍵の生成において基にされた配信復号鍵が暴露された場合に、前記配信暗号鍵を前記リポークリスト手段に書き込む登録手段とを含み、

ここで、前記送信装置は、新たにデジタル著作物であるコンテンツを送信し、

前記配信鍵取得手段は、新たに配信暗号鍵を取得し、取得した配信暗号鍵がリポークリスト手段に書き込まれているか否かを判断し、書き込まれていると判断する場合には、前記暗号化手段に対して暗号化を禁止し、前記送信手段に対して送信を禁止する

ことを特徴とする請求項 7 に記載の送信装置。

【請求項 9】

前記記憶手段は、さらに、前記デジタル著作物の利用条件を示す利用条件情報を記憶しており、

前記送信手段は、さらに、前記記憶手段から前記利用条件情報を読み出し、読み出した前記利用条件情報にハッシュアルゴリズムを施してハッシュ値を生成し、生成した前記ハッシュ値と読み出した利用条件情報を、セキュアにネットワークを介して送信する

ことを特徴とする請求項 6 に記載の送信装置。

【請求項 10】

前記送信装置は、さらに、

前記記録媒体装置との間で相互に機器の正当性を認証する認証手段を含み、

前記配信暗号鍵取得手段は、前記認証に成功した場合にのみ、前記配信暗号鍵を前記記録媒体装置から取得し、

前記暗号化手段は、前記認証に成功した場合にのみ、暗号化し、
前記送信手段は、前記認証に成功した場合にのみ、送信する
ことを特徴とする請求項 6 に記載の送信装置。

【請求項 1 1】

前記送信装置は、さらに、
前記記録媒体装置が備える耐タンパモジュール部を更新するための更新情報を予め記憶している更新情報記憶手段と、
前記更新情報記憶手段から前記更新情報を読み出し、読み出した前記更新情報を、ネットワーク及び受信装置を介して、前記記録媒体装置へ送信する更新情報送信手段と
を含むことを特徴とする請求項 6 に記載の送信装置。

【請求項 1 2】

前記送信装置は、さらに、
前記更新情報記憶手段から前記更新情報を読み出し、読み出した更新情報にハッシュアルゴリズムを施してハッシュ値を生成し、生成したハッシュ値を、ネットワーク及び受信装置を介して、前記記録媒体装置へセキュアに送信するハッシュ手段
を含むことを特徴とする請求項 1 1 に記載の送信装置。

【請求項 1 3】

前記更新情報記憶手段が記憶している更新情報は、前記耐タンパモジュール部が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含み、
前記更新情報送信手段は、前記耐タンパモジュール部が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含む前記更新情報を読み出し、読み出した前記更新情報を送信することを特徴とする請求項 1 2 に記載の送信装置。

【請求項 1 4】

送信装置から送信されたデジタル 情報 を、受信装置を介して、記録する可搬型の記録媒体装置であって、
前記記録媒体装置が前記受信装置に装着され、
前記送信装置は、デジタル 情報 である原コンテンツを配信暗号鍵に基づいて暗号化して第 1 暗号化情報を生成し、生成した第 1 暗号化情報を、ネットワークを介して、前記受信装置へ送信し、
前記記録媒体装置は、
情報を記憶するための領域を備える情報記憶手段と、
耐タンパ性を有する耐タンパモジュール手段とを備え、
前記耐タンパモジュール手段は、
配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶している鍵記憶部と、
前記受信装置を介して、送信された前記第 1 暗号化情報を取得する取得部と、
前記配信復号鍵に基づいて前記第 1 暗号化情報を復号して中間情報を生成する復号部と

、
前記媒体固有鍵に基づいて前記中間情報を暗号化して第 2 暗号化情報を生成する暗号化部と、
生成した第 2 暗号化情報を前記情報記憶手段に書き込む書込部と
を備えることを特徴とする記録媒体装置。

【請求項 1 5】

前記送信装置は、前記デジタル 情報 として、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第 1 暗号化情報を生成し、生成した第 1 暗号化情報を、ネットワークを介して、前記受信装置へ送信し、
前記記録媒体装置は、前記受信装置を介して、前記第 1 暗号化情報を取得することを特徴とする請求項 1 4 に記載の記録媒体装置。

【請求項 1 6】

前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第1暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ及び第1暗号化コンテンツ鍵を含む前記第1暗号化情報を送信し、

前記取得部は、出力された前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を含む前記第1暗号化情報を取得し、

前記復号部は、前記配信復号鍵を用いて、前記第1暗号化情報に含まれる前記第1暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記第1暗号化情報に含まれる前記暗号化コンテンツ及び生成した前記中間コンテンツ鍵を含む前記中間情報を生成し、

前記暗号化部は、前記媒体固有鍵を用いて、前記中間情報に含まれる前記中間コンテンツ鍵を暗号化して第2暗号化コンテンツ鍵を生成し、前記中間情報に含まれる前記暗号化コンテンツ及び生成した前記第2暗号化コンテンツ鍵を含む前記第2暗号化情報を生成し、

前記書込部は、前記暗号化コンテンツ及び前記第2暗号化コンテンツ鍵を含む前記第2暗号化情報を書き込む

ことを特徴とする請求項15に記載の記録媒体装置。

【請求項17】

前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第1暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第1暗号化利用条件情報を生成し、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を、ネットワークを介して、前記受信装置へ送信し、

前記取得部は、さらに、前記受信装置を介して、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を取得し、

前記復号部は、さらに、前記配信復号鍵を用いて、前記第1暗号化利用条件鍵を復号して中間利用条件鍵を生成し、生成した前記中間利用条件鍵を用いて、前記第1暗号化利用条件情報を復号して、中間利用条件情報を生成し、

前記暗号化部は、さらに、前記媒体固有鍵を用いて、前記中間利用条件情報を暗号化して第2暗号化利用条件情報を生成し、

前記書込部は、さらに、生成した第2暗号化利用条件情報を前記情報記憶手段に書き込む

ことを特徴とする請求項16に記載の記録媒体装置。

【請求項18】

前記送信装置は、さらに、秘密鍵である配信用復号鍵を基にして公開鍵生成アルゴリズムを用いて生成された公開鍵である前記配信暗号鍵を取得し、公開鍵である配信暗号鍵を用いて、公開鍵暗号アルゴリズムにより、暗号化し、

前記復号部は、公開鍵復号アルゴリズムにより、前記配信用復号鍵を用いて復号する

ことを特徴とする請求項17に記載の記録媒体装置。

【請求項19】

前記耐タンパモジュール手段は、さらに、

前記復号部により生成された配信データ形式である前記中間情報を変換して、記録データ形式の記録中間情報を生成する変換部を含み、

前記暗号化部は、前記中間情報に代えて、前記記録中間情報を暗号化する

ことを特徴とする請求項16に記載の記録媒体装置。

【請求項20】

前記送信装置は、前記記録媒体装置が備える前記耐タンパモジュール手段を更新するための更新情報を予め記憶しており、前記更新情報を読み出し、読み出した前記更新情報を、ネットワーク及び受信装置を介して、前記記録媒体装置へ送信し、

前記耐タンパモジュール手段は、マイクロプロセッサとコンピュータプログラムを記録している半導体メモリを含み、前記コンピュータプログラムに従って、前記マイクロプロセッサが動作することにより、前記耐タンパモジュール手段に含まれる構成要素が動作し

、
前記取得部は、前記受信装置を介して、前記更新情報を取得し、

前記耐タンパモジュール手段は、さらに、取得した前記更新情報を用いて、前記コンピュータプログラムを更新し、これにより、前記耐タンパモジュール手段に含まれる構成要素が更新される更新部を含む

ことを特徴とする請求項 19 に記載の記録媒体装置。

【請求項 21】

前記送信装置は、さらに、前記更新情報を読み出し、読み出した更新情報にハッシュアルゴリズムを施して第1ハッシュ値を生成し、生成した第1ハッシュ値を、ネットワーク及び受信装置を介して、前記記録媒体装置へセキュアに送信し、

前記耐タンパモジュール手段は、さらに、

取得した前記更新情報に前記ハッシュアルゴリズムを施して第2ハッシュ値を生成するハッシュ部と、

取得した前記第1ハッシュ値と生成した前記第2ハッシュ値とが一致するか否かを判断する比較判断部とを含み、

前記更新部は、前記比較判断部により一致すると判断された場合にのみ、更新する

ことを特徴とする請求項 20 に記載の記録媒体装置。

【請求項 22】

前記送信装置が記憶している更新情報は、前記耐タンパモジュール手段が備える暗号化方式、復号方式、又は配信データ形式から記録データ形式へのデータ変換方式を更新するための情報を含み、前記前記更新情報を送信し、

前記取得部は、暗号化方式、復号方式、又はデータ変換方式を更新するための前記更新情報を前記受信装置を介して取得し、

前記更新部は、取得した前記更新情報を用いて、前記コンピュータプログラムを更新し、これにより、前記耐タンパモジュール手段に含まれる暗号化部、復号部、又は変換部が更新される

ことを特徴とする請求項 21 に記載の記録媒体装置。

【請求項 23】

前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報を記憶しており、前記利用条件情報を読み出し、読み出した前記利用条件情報にハッシュアルゴリズムを施して第1ハッシュ値を生成し、生成した前記第1ハッシュ値と読み出した利用条件情報を、ネットワークを介してセキュアに送信し、

前記取得部は、さらに、前記受信装置を介して、送信された前記第1ハッシュ値と前記利用条件情報とを取得し、

前記耐タンパモジュール手段は、さらに、

取得した前記利用条件情報に前記ハッシュアルゴリズムを施して第2ハッシュ値を生成するハッシュ部と、

取得した前記第1ハッシュ値と生成した前記第2ハッシュ値とが一致するか否かを判断する比較判断部とを含み、

前記暗号化部は、前記比較判断部により一致すると判断された場合にのみ、暗号化し、

前記書込部は、前記比較判断部により一致すると判断された場合にのみ、書き込む

ことを特徴とする請求項 16 に記載の記録媒体装置。

【請求項 24】

前記送信装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証し、前記認証に成功した場合にのみ、前記配信暗号鍵を前記記録媒体装置から取得し、暗号化し、送信し、

前記耐タンパモジュール手段は、さらに、前記送信装置との間で相互に機器の正当性を

認証する認証手段を含み、

前記取得部は、前記認証に成功した場合にのみ、取得し、
前記復号部は、前記認証に成功した場合にのみ、復号し、
前記暗号化部は、前記認証に成功した場合にのみ、暗号化し、
前記書込部は、前記認証に成功した場合にのみ、書き込む
ことを特徴とする請求項 1 6 に記載の記録媒体装置。

【請求項 2 5】

前記記録媒体装置は、再生装置に装着され、前記再生装置は、前記情報記憶手段から情報を読み出す、

前記耐タンパモジュール手段は、さらに、前記再生装置との間で相互に機器の正当性を認証し、前記認証に成功した場合にのみ、前記再生装置に対して情報の読み出しを許可する認証手段を含む

ことを特徴とする請求項 1 6 に記載の記録媒体装置。

【請求項 2 6】

前記復号部は、複数の復号方式を予め備えており、前記複数の復号方式から選択した 1 個の復号方式を用いて、復号し、ここで、選択した前記復号方式は、前記送信装置で用いられる暗号化方式の逆変換を行う

ことを特徴とする請求項 1 6 に記載の記録媒体装置。

【請求項 2 7】

前記暗号化部は、複数の暗号化方式を予め備えており、前記複数の暗号化方式から選択した 1 個の暗号方式を用いて、暗号化する

ことを特徴とする請求項 1 6 に記載の記録媒体装置。

【請求項 2 8】

前記鍵記憶部は、複数の配信復号鍵候補を記憶しており、前記複数の配信復号鍵候補から 1 個の配信復号鍵候補が前記配信復号鍵として選択されており、

前記復号部は、選択された前記配信復号鍵を用いる

ことを特徴とする請求項 1 6 に記載の記録媒体装置。

【請求項 2 9】

前記耐タンパモジュール手段は、ソフトウェア、ハードウェア、又はソフトウェア及びハードウェアの組合せにより、耐タンパ性を実現している

ことを特徴とする請求項 1 6 に記載の記録媒体装置。

【請求項 3 0】

前記送信装置は、前記デジタル情報として、コンテンツ鍵と利用条件の少なくとも一方を配信暗号鍵に基づいて暗号化して第 1 暗号化情報を生成し、生成した第 1 暗号化情報を、ネットワークを介して、前記受信装置へ送信し、

前記記録媒体装置は、前記受信装置を介して、前記第 1 暗号化情報を取得する

ことを特徴とする請求項 1 4 に記載の記録媒体装置。

【請求項 3 1】

前記耐タンパモジュール手段は、さらに、

前記復号部により生成された配信データ形式である前記中間情報を変換して、記録データ形式の記録中間情報を生成する変換部を含み、

前記暗号化部は、前記中間情報に代えて、前記記録中間情報を暗号化する

ことを特徴とする請求項 3 0 に記載の記録媒体装置。

【請求項 3 2】

送信装置からネットワーク及び受信装置を介して送信されて可搬型の記録媒体装置に書き込まれたデジタル情報を再生する再生装置であって、

前記記録媒体装置が前記受信装置に装着され、

前記送信装置は、デジタル情報を配信暗号鍵に基づいて暗号化して第 1 暗号化情報を生成し、生成した第 1 暗号化情報をネットワークを介して前記受信装置へ送信し、

前記記録媒体装置は、情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タ

ンパモジュール部とを備え、前記耐タンパモジュール部は、前記受信装置を介して送信された前記第1暗号化情報を取得し、配信復号鍵に基づいて前記第1暗号化情報を復号して中間情報を生成し、前記記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第2暗号化情報を生成し、生成した第2暗号化情報を前記情報記憶領域に書き込む、

ここで、前記第2暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、

前記再生装置は、

前記記録媒体装置から前記媒体固有鍵をセキュアに取得する鍵取得手段と、

前記情報記憶領域から前記第2暗号化情報を読み出す読出手段と、

取得した前記媒体固有鍵に基づいて、読み出した前記第2暗号化を復号して、復号デジタル情報を生成する復号手段と

を備えることを特徴とする再生装置。

【請求項33】

前記送信装置は、デジタル情報として、デジタル著作物である原コンテンツを暗号化して第1暗号化情報を生成し、

前記復号手段は、取得した前記媒体固有鍵に基づいて、読み出した前記第2暗号化を復号して、前記復号デジタル情報として、復号コンテンツを生成し、

前記再生装置は、さらに、生成された復号コンテンツを再生する再生手段を備えることを特徴とする請求項32に記載の再生装置。

【請求項34】

前記送信装置は、原コンテンツと当該原コンテンツに固有の原コンテンツ鍵とを予め記憶しており、デジタル著作物の配信のために用いられる配信暗号鍵を取得し、前記原コンテンツ鍵を用いて、原コンテンツを暗号化して暗号化コンテンツを生成し、取得した配信暗号鍵を用いて、前記原コンテンツ鍵を暗号化して第1暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツと第1暗号化コンテンツ鍵とを含む前記第1暗号化情報を送信し、

前記耐タンパモジュール部は、前記配信復号鍵及び前記記録媒体装置に固有の媒体固有鍵を予め記憶しており、出力された前記暗号化コンテンツ及び前記第1暗号化コンテンツ鍵を含む前記第1暗号化情報を取得し、前記配信復号鍵を用いて、前記第1暗号化コンテンツ鍵を復号して中間コンテンツ鍵を生成し、前記媒体固有鍵を用いて、生成した前記中間コンテンツ鍵を暗号化して第2暗号化コンテンツ鍵を生成し、取得した前記暗号化コンテンツと生成した前記第2暗号化コンテンツ鍵とを含む前記第2暗号化情報を書き込み、

前記読出手段は、前記暗号化コンテンツと前記第2暗号化コンテンツ鍵とを含む前記第2暗号化情報を読み出し、

前記復号手段は、取得した前記媒体固有鍵を用いて、読み出した前記第2暗号化コンテンツ鍵を復号して、復号コンテンツ鍵を生成し、生成した復号コンテンツ鍵を用いて、読み出した前記暗号化コンテンツを復号して復号コンテンツを生成する

ことを特徴とする請求項33に記載の再生装置。

【請求項35】

前記送信装置は、さらに、前記デジタル著作物の利用条件を示す利用条件情報と、前記利用条件情報に固有の原利用条件鍵とを記憶しており、前記配信暗号鍵を用いて、前記原利用条件鍵を暗号化して第1暗号化利用条件鍵を生成し、前記原利用条件鍵を用いて、前記利用条件情報を暗号化して第1暗号化利用条件情報を生成し、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を、ネットワークを介して、前記受信装置へ送信し、

前記記録媒体装置は、さらに、前記受信装置を介して、前記第1暗号化利用条件鍵及び前記第1暗号化利用条件情報を取得し、前記配信復号鍵を用いて、前記第1暗号化利用条件鍵を復号して中間利用条件鍵を生成し、生成した前記中間利用条件鍵を用いて、前記第1暗号化利用条件情報を復号して、中間利用条件情報を生成し、前記媒体固有鍵を用いて、前記中間利用条件情報を暗号化して第2暗号化利用条件情報を生成し、生成した第2暗

号化利用条件情報を前記情報記憶領域に書き込み、

前記読出手段は、さらに、前記情報記憶領域から前記第2暗号化利用条件情報を読み出し、

前記復号手段は、さらに、前記媒体固有鍵に基づいて、読み出した前記第2暗号化利用条件情報を復号して復号利用条件情報を生成し、

前記再生手段は、さらに、生成された復号利用条件情報に基づいて復号コンテンツの再生の可否を判断し、再生可と判断される場合にのみ、前記生成された復号コンテンツを再生する

ことを特徴とする請求項34に記載の再生装置。

【請求項36】

前記利用条件情報は、前記復号コンテンツの再生回数を制限する情報、前記復号コンテンツの再生期間を制限する情報、又は前記復号コンテンツの再生累積時間を制限する情報を含み、

前記再生手段は、再生回数を制限する情報、再生期間を制限する情報、又は再生累積時間を制御する情報に基づいて復号コンテンツの再生の可否を判断する

ことを特徴とする請求項35に記載の再生装置。

【請求項37】

前記再生装置は、さらに、前記記録媒体装置との間で相互に機器の正当性を認証する認証手段を含み、

前記鍵取得手段は、前記認証に成功した場合にのみ、取得し、

前記読出手段は、前記認証に成功した場合にのみ、読み出す

ことを特徴とする請求項34に記載の再生装置。

【請求項38】

前記送信装置は、前記デジタル情報として、コンテンツ鍵と利用条件の少なくとも一方を配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報を、ネットワークを介して、前記受信装置へ送信し、

前記記録媒体装置は、前記受信装置を介して、前記第1暗号化情報を取得し、

前記復号手段は、取得した前記媒体固有鍵に基づいて、読み出した前記第2暗号化を復号して、コンテンツ鍵と利用条件の少なくとも一方である前記復号デジタル情報を生成する

ことを特徴とする請求項32に記載の再生装置。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0008

【補正方法】変更

【補正の内容】

【0008】

このような問題点を解決するために、従来、パソコン内のコンピュータプログラムに、本来不要な命令や分岐命令をあらかじめ含ませておいて、ハッキングが困難になるようにしている。しかしながら、プログラムの増大を招き、また速度性能が低下するという問題点がある。

本発明は、上述した問題点を解決するために、プログラムの量が増加することなく、また速度性能が低下することなく、上述のようなハッキングを困難にするデジタル情報保護システム、記録媒体装置、送信装置及び再生装置を提供することを目的とする。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正の内容】

【0009】

【課題を解決するための手段】

上記目的を達成するために、本発明は、送信装置から送信されたデジタル情報を、受信装置を介して、可搬型の記録媒体装置に書き込み、再生装置により再生するデジタル情報保護システムであって、前記デジタル情報保護システムは、デジタル情報を配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報をネットワークを介して送信する前記送信装置を含み、ここで、前記記録媒体装置が前記受信装置に装着され、前記デジタル情報保護システムは、さらに、ネットワークを介して前記第1暗号化情報を受信し、受信した前記第1暗号化情報を前記記録媒体装置へ出力する受信装置と、情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タンパモジュール部とを備える前記記録媒体装置とを含み、前記耐タンパモジュール部は、出力された前記第1暗号化情報を取得し、配信復号鍵に基づいて前記第1暗号化情報を復号して中間情報を生成し、前記記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第2暗号化情報を生成し、生成した第2暗号化情報を前記情報記憶領域に書き込み、ここで、前記第2暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、前記デジタル情報保護システムは、さらに、前記情報記憶領域から前記第2暗号化情報を読み出し、前記媒体固有鍵をセキュアに読み出し、前記媒体固有鍵に基づいて前記第2暗号化情報を復号して復号デジタル情報を生成し、生成した復号デジタル情報を再生する前記再生装置を含むことを特徴とする。

また、本発明は、送信装置から送信されたデジタル著作物を、受信装置を介して、可搬型の記録媒体装置に書き込み、再生装置により再生するデジタル著作物保護システムであって、前記デジタル著作物保護システムは、デジタル著作物である原コンテンツを配信暗号鍵に基づいて暗号化して第1暗号化情報を生成し、生成した第1暗号化情報をネットワークを介して送信する前記送信装置を含み、ここで、前記記録媒体装置が前記受信装置に装着され、前記デジタル著作物保護システムは、さらに、ネットワークを介して前記第1暗号化情報を受信し、受信した前記第1暗号化情報を前記記録媒体装置へ出力する受信装置と、情報を記憶するための情報記憶領域と、耐タンパ性を有する耐タンパモジュール部とを備える前記記録媒体装置とを含み、前記耐タンパモジュール部は、出力された前記第1暗号化情報を取得し、配信復号鍵に基づいて前記第1暗号化情報を復号して中間情報を生成し、前記記録媒体装置に固有の媒体固有鍵に基づいて前記中間情報を暗号化して第2暗号化情報を生成し、生成した第2暗号化情報を前記情報記憶領域に書き込み、ここで、前記第2暗号化情報が書き込まれた前記記録媒体装置が前記再生装置に装着され、前記デジタル著作物保護システムは、さらに、前記情報記憶領域から前記第2暗号化情報を読み出し、前記媒体固有鍵をセキュアに読み出し、前記媒体固有鍵に基づいて前記第2暗号化情報を復号して復号コンテンツを生成し、生成した復号コンテンツを再生する前記再生装置を含むことを特徴とする。